# Cisco Digital Network Architecture Center 어플라이언스 설치 가이드, 릴리스 1.2.10(M4 섀시)

초판: 2019년 1월 29일

최종 변경: 2019년 2월 21일

**Americas Headquarters**
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

이 설명서의 제품 관련 사양 및 정보는 예고 없이 변경될 수 있습니다. 이 설명서의 모든 설명, 정보 및 권장 사항이 정확하다고 판단되더라도 어떠한 형태의 명시적이거나 묵시적인 보증도 하지 않습니다. 모든 제품의 해당 애플리케이션에 대한 사용은 전적으로 사용자에게 책임이 있습니다.

동봉한 제품의 소프트웨어 라이선스 및 제한된 보증은 제품과 함께 제공된 정보 패킷에 설명되어 있으며 본 문서에 참조를 통해 포함됩니다. 소프트웨어 라이선스 또는 제한 보증을 찾을 수 없는 경우 CISCO 담당자에게 사본을 요청하십시오.

Cisco의 TCP 헤더 압축은 UNIX 운영 체제의 UCB 퍼블릭 도메인 버전의 일부로서 University of Berkeley(UCB)에서 개발된 프로그램을 적용하여 구현합니다. All rights reserved. Copyright © 1981, Regents of the University of California.

여기에 명시된 다른 모든 보증에도 불구하고 이러한 공급자의 모든 문서 파일 및 소프트웨어는 모든 결점을 포함하여 "있는 그대로" 제공됩니다. CISCO 및 위에 언급된 모든 공급자는 상품성, 특정 목적에의 적합성, 타인의 권리 비침해 또는 처리, 사용, 거래 행위로 발생하는 문제에 대한 묵시적 보증을 포함하여(단, 이에 한하지 않음) 묵시적이든 명시적이든 모든 종류의 보증을 부인합니다.

CISCO 또는 그 공급업체는 이 설명서의 사용 또는 사용할 수 없음으로 인한 모든 파생적, 부수적, 직접, 간접, 특별, 징벌적 또는 기타 모든 손해(영업 이익 손실, 영업 중단, 영업 정보 손실, 또는 그 밖의 금전적 손실로 인한 손해를 포함하되 이에 제한되지 않음)에 대하여 어떠한 경우에도 책임을 지지 않으며, 이는 CISCO 또는 그 공급업체가 그와 같은 손해의 가능성을 사전에 알고 있던 경우에도 마찬가지입니다.

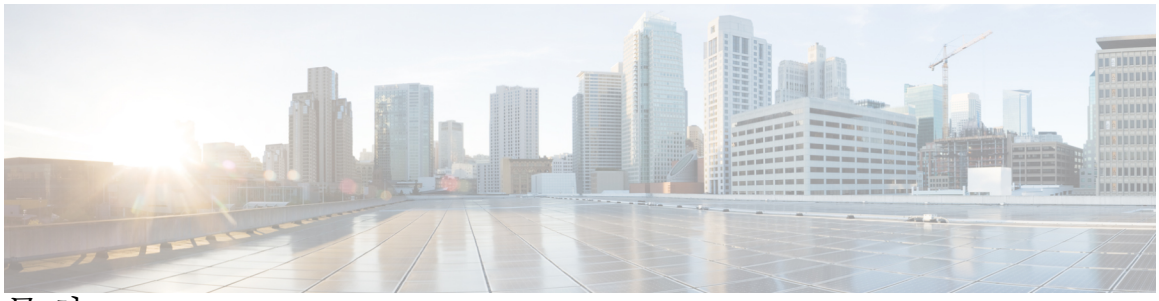
이 문서에서 사용된 모든 IP(인터넷 프로토콜) 주소와 전화 번호는 실제 주소와 전화 번호가 아닙니다. 이 문서에 포함된 예, 명령 표시 출력, 네트워크 토폴로지 다이어그램 및 다른 그림은 이해를 돕기 위한 자료일 뿐이며, 실제 IP 주소나 전화 번호가 사용되었다면 이는 의도하지 않은 우연의 일치입니다.

모든 인쇄된 사본 및 이 문서의 중복된 소프트 복사본은 제어 대상이 아닌 것으로 간주됩니다. 최신 버전에 대한 현재 온라인 버전을 참조하십시오.

Cisco는 전 세계에 200개가 넘는 지사를 운영하고 있습니다. 각 지사의 주소 및 전화번호는 Cisco 웹사이트(www.cisco.com/go/office)에서 확인하십시오.

Cisco 및 Cisco 로고는 미국 및 기타 국가에서 Cisco Systems, Inc. 및/또는 계열사의 상표 또는 등록 상표입니다. Cisco 상표 목록을 확인하려면 www.cisco.com go trademarks로 이동하십시오. 언급된 타사 상표는 해당 소유권자의 재산입니다. '파트너'라는 용어의 사용이 Cisco와 다른 회사 간의 파트너십 관계를 의미하는 것은 아닙니다. (1721R)

© 2019 Cisco Systems, Inc. 모든 권리 보유.



# 목 차


장 1 어플라이언스 기능 검토 1

기능 요약 1

전면 패널 및 후면 패널 2

제품 외장 사양 10

환경 사양 11

전원 사양 11

장 2 구축 계획 13

워크플로 계획 13

Cisco DNA Center 및 소프트웨어 정의 액세스 정보 14

인터페이스 케이블 연결 15

필수 서브넷 및 추가 IP 주소 17

인터페이스 이름 및 마법사 구성 순서 20

필수 인터넷 URL 및 FQDN(Fully Qualified Domain Name) 21

인터넷에 대한 보안 액세스 제공 23

필수 네트워크 포트 24

필수 SD-Access 포트 및 프로토콜 26

필수 구성 정보 34

필수 초기 설정 정보 36

장 3 어플라이언스 설치 39

어플라이언스 설치 워크플로 39

어플라이언스 포장 풀기 및 검사 40

설치 경고 및 지침 검토 41

랙 요건 검토 42
어플라이언스 연결 및 전원 켜기 42
LED 확인 43

장 4 어플라이언스 구성 47
어플라이언스 구성 워크플로 47
CIMC에 대한 브라우저 액세스 활성화 48
사전 검사 실행 53
Cisco DNA Center ISO 이미지 확인 60
부팅 가능 USB 드라이브 생성 61
어플라이언스 이미지 재설치 62
Cisco DNA Center ISO 이미지 설치 64
마스터 노드 구성 64
추가 기능 노드 구성 78
고가용성 클러스터 구축 시나리오 93
새 HA 구축 94
표준 인터페이스 구성을 사용하는 마스터 노드의 기존 HA 구축 94
비표준 인터페이스 구성을 사용하는 마스터 노드의 기존 HA 구축 95
추가 HA 구축 고려사항 95
원격 측정 95
무선 컨트롤러 96
최신 Cisco DNA Center 릴리스로 업그레이드 96

장 5 초기 설정 완료 97
초기 설정 워크플로 97
호환 가능 브라우저 98
최초 로그인 98
Cisco ISE 통합 Cisco DNA Center 107
인증 및 정책 서버 구성 109
SNMP 속성 구성 111
서비스 재배포 111

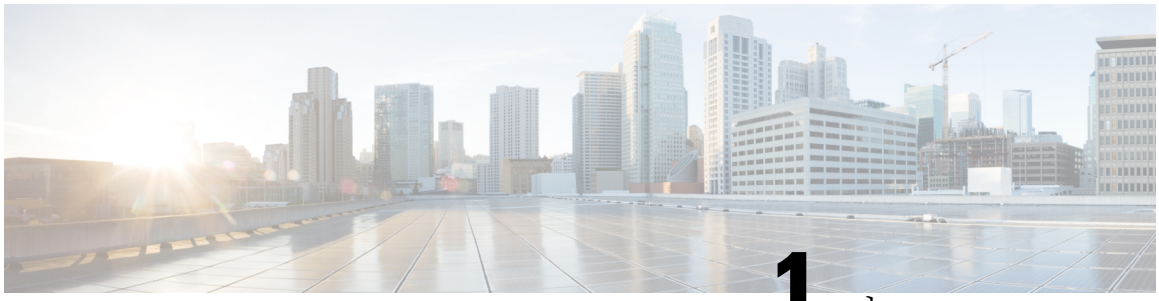
장 6 구축 트러블슈팅 113

트러블슈팅 작업 113

로그아웃 113

구성 마법사를 사용하여 어플라이언스 재구성 114

어플라이언스의 전원 껐다 켜기 115



1 장

# 어플라이언스 기능 검토


- 기능 요약, 1 페이지
- 전면 패널 및 후면 패널, 2 페이지
- 제품 외장 사양, 10 페이지
- 환경 사양, 11 페이지
- 전원 사양, 11 페이지


## 기능 요약

Cisco에서는 랙 마운트형 어플라이언스(Cisco 부품 번호 DN1-HW-APL)의 형태로 Cisco DNA Center를 제공합니다. 이 어플라이언스는 Cisco UCS C220 M4 섀시로 구성됩니다(mLOM 슬롯에는 VIC(Virtual Interface Card) 1227이 추가됨). Cisco DNA Center 소프트웨어 이미지는 어플라이언스에 사전 설치되어 있지만 사용하기 위해서는 구성해야 합니다.

다음 표에는 어플라이언스 기능이 요약되어 있습니다.

표 ***1: Cisco DNA Center*** 어플라이언스 시리즈 기능

| 기능 | 설명 |
|---|---|
| 섀시 | 1RU(1개 랙 장치) 섀시가 제공됩니다. |
| 프로세서 | 최대 2개의 Intel Xeon CPU E5-2699 2.20GHz v4 Series 프로세서 제품군 CPU |
| 메모리 | 등록된 DIMM(RDIMM) 또는 로드 감소 DIMM(LRDIMM)용 24개 슬롯(각 CPU당 12개) |
| 스토리지 | 2.5인치 SFF(소형 폼 팩터) SSD(Solid State Drive) 8개 |
| 디스크 관리(RAID) | 사전 구성된 3개의 RAID 설정: 슬롯 1 및 2의 RAID 1, 슬롯 3 및 4의 RAID 1, 슬롯 5, 6, 7, 8의 RAID 10. 이러한 설정은 사용자가 구성할 수 없습니다. |

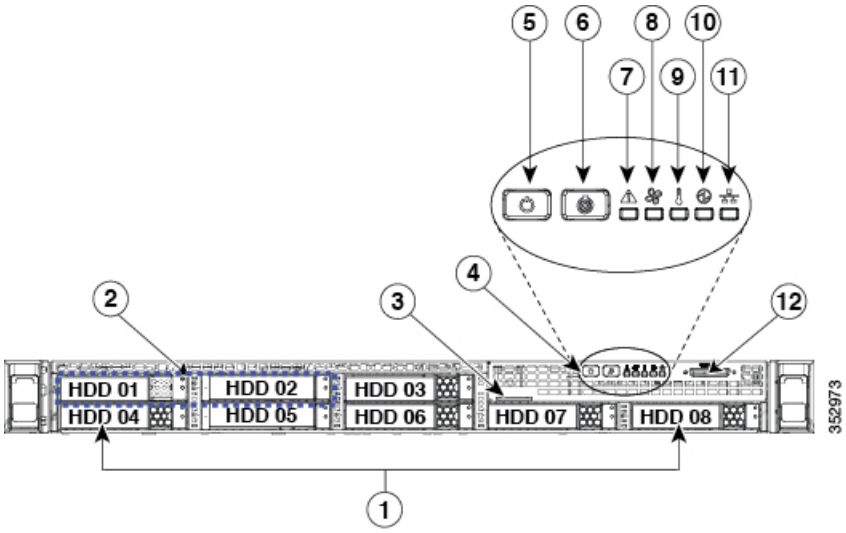
| 기능 | 설명 |
|---|---|
| 네트워크 및 관리 I/O | 지원되는 커넥터:<br>• Cisco UCS VIC(Virtual Interface Card) 1227의 10Gbps 이더넷 포트 2개<br>• 1Gbps 이더넷 전용 관리 포트 1개<br>• 1Gbps BASE-T 이더넷 LAN 포트 2개<br>다음 커넥터는 사용할 수 있지만 일반적으로 Cisco DNA Center의 일상적인 작업에는 사용되지 않습니다.<br>• RS-232 시리얼 포트(RJ-45 커넥터) 1개<br>• 15핀 VGA 커넥터 1개<br>• USB 3.0 커넥터 2개<br>• USB 2.0 2개, VGA 1개, 시리얼(DB-9) 커넥터 1개를 제공하는 KVM 케이블과 함께 사용되는 전면 패널 KVM 커넥터 1개 |
| 전원 | 듀얼 AC 전력 공급 장치(각 770W AC)<br>서버에서 여러 전력 공급 장치 유형 또는 전력 등급을 혼합하여 사용하지 마십시오.<br>1+1 이중화. |
| 냉각 | 전후면 냉각용 핫 스왑 가능 팬 모듈 6개. |
| 비디오 | 60Hz에서 최대 1920 x 1200, 16bpp의 VGA 비디오 해상도 및 최대 256MB의 비디오 메모리 제공. |

# 전면 패널 및 후면 패널

다음 그림 및 표에는 Cisco UCS C220 M4 새시가 있는 Cisco DNA Center 어플라이언스의 전면 및 후면 패널에 대해 설명되어 있습니다.

어플라이언스 전면 및 후면 패널과 어플라이언스 NIC의 케이블 연결 방식을 설명하는 짧은 비디오를 보려면 이 링크를 클릭합니다.

그림 *1:* 어플라이언스 전면 패널

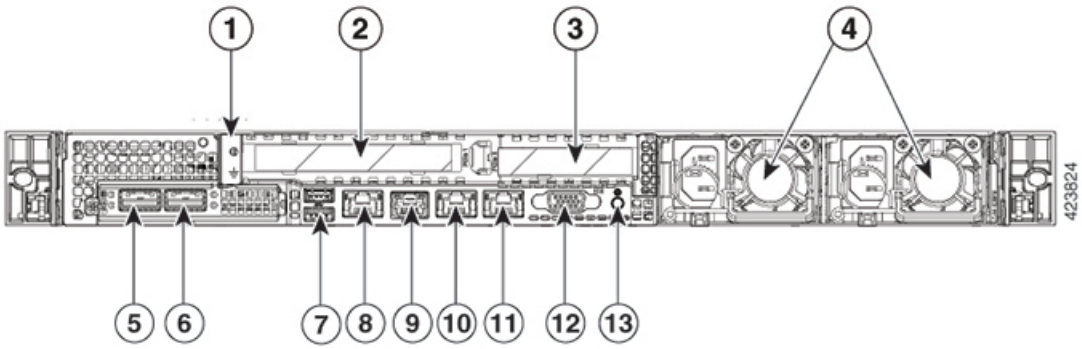



| **Component**(구성 요소) | 설명 |
|---|---|
| 1 | 2.5인치 SDD 드라이브 8개. 설치된 각 드라이브 베이에는 결함 LED와 활동 LED가 있습니다.<br>드라이브 결함 LED가 다음과 같은 경우:<br>• 꺼짐 - 드라이브가 정상적으로 작동하고 있습니다.<br>• 황색 - 드라이브에 장애가 발생했습니다.<br>• 황색, 깜박임 - 드라이브를 다시 구축하는 중입니다.<br>드라이브 활동 LED가 다음과 같은 경우:<br>• 꺼짐 - 슬레드에 하드 드라이브가 없습니다(액세스 없음, 결함 없음).<br>• 녹색 - 드라이브가 준비된 상태입니다.<br>• 녹색(깜박임) - 드라이브에서 데이터를 읽거나 쓰는 중입니다. |
| 2 | 드라이브 베이 1 및 2에서는 SAS/SATA 및 NVMe PCIe SSD(Solid State Drive)를 지원합니다. 결함 및 활동 LED와 해당 상태는 설치된 2.5인치 SDD 드라이브와 동일합니다. |
| 3 | 풀아웃 자산 태그 |
| 4 | 작업 하위 패널 버튼 및 LED. 이러한 버튼의 LED 상태 및 표시되는 조건은 다음 항목에 설명되어 있습니다. |

| **Component(**구성 요소**)** | 설명 |
|---|---|
| 5 | 전원 버튼/전원 상태 LED. LED가 다음과 같은 경우:<br>• 꺼짐 - 어플라이언스에 AC 전원이 없습니다.<br>• 황색 - 어플라이언스가 예비 전원 모드입니다. 전원이 CIMC 및 일부 마더보드 기능에만 공급됩니다.<br>• 녹색 - 어플라이언스가 주 전원 모드입니다. 전원이 모든 서버 구성 요소에 공급됩니다. |
| 6 | 유닛 식별 버튼 및 LED. LED가 다음과 같은 경우:<br>• 파란색 - 유닛 식별이 활성 상태입니다.<br>• 꺼짐 - 유닛 식별이 비활성 상태입니다. |
| 7 | 시스템 상태 LED. LED가 다음과 같은 경우:<br>• 녹색 - 어플라이언스가 정상적으로 작동하고 있습니다.<br>• 녹색, 깜박임 - 어플라이언스에서 시스템 초기화 및 메모리 검사를 실시하고 있습니다.<br>• 황색, 계속 켜져 있음 - 어플라이언스가 성능이 저하된 상태로 작동 중이며, 다음 중 하나 이상이 그 이유일 수 있습니다.<br>  • 전원 공급 장치 이중화에 문제가 생겼습니다.<br>  • CPU가 불일치 상태입니다.<br>  • 하나 이상의 CPU에 결함이 있습니다.<br>  • 하나 이상의 DIMM에 결함이 있습니다.<br>  • RAID 컨피그레이션에서 하나 이상의 드라이브에 장애가 발생했습니다.<br>• 황색, 깜박임 - 어플라이언스가 중대한 결함 상태이며, 다음 중 하나 이상이 그 이유일 수 있습니다.<br>  • 부팅에 실패했습니다.<br>  • 치명적인 CPU 및/또는 버스 오류가 탐지되었습니다.<br>  • 서버가 과열 상태입니다. |

| **Component(**구성 요소**)** | 설명 |
|---|---|
| 8 | 팬 상태 LED. LED가 다음과 같은 경우:<br>• 녹색 - 모든 팬 모듈이 정상적으로 작동하고 있습니다.<br>• 황색, 계속 켜져 있음 - 하나의 팬 모듈에 장애가 발생했습니다.<br>• 황색, 깜박임 - 심각한 장애, 두 개 이상의 팬 모듈에 장애가 발생했습니다. |
| 9 | 온도 상태 LED. LED가 다음과 같은 경우:<br>• 녹색 - 어플라이언스가 정상 온도로 작동하고 있습니다.<br>• 황색, 계속 켜져 있음 - 하나 이상의 온도 센서가 경고 임계값을 초과했습니다.<br>• 황색(깜박임) - 하나 이상의 온도 센서에서 중요 임계값이 초과되었습니다. |
| 10 | 전력 공급 장치 상태 LED. LED가 다음과 같은 경우:<br>• 녹색 - 모든 전력 공급 장치가 정상적으로 작동하고 있습니다.<br>• 황색, 계속 켜져 있음 - 하나 이상의 전력 공급 장치가 성능이 저하된 상태로 작동 중입니다.<br>• 황색, 깜박임 - 하나 이상의 전력 공급 장치에 중대한 결함이 있습니다. |
| 11 | 네트워크 링크 활동 LED. LED가 다음과 같은 경우:<br>• 녹색, 깜박임 - 하나 이상의 이더넷 LOM 포트가 링크 활성 상태이며 활동이 있습니다.<br>• 녹색 - 하나 이상의 이더넷 LOM 포트가 링크 활성 상태이지만 활동이 없습니다.<br>• 꺼짐 - 이더넷 링크가 유휴 상태입니다. |
| 12 | KVM 커넥터. USB 2.0 2개, VGA 1개, 시리얼 커넥터 1개를 제공하는 KVM 케이블과 함께 사용됩니다. |

그림 *2:* 어플라이언스 후면 패널




| **Component**(구성 요소) | 설명 |
|---|---|
| 1 | 접지 러그 홀(DC 전원 공급 장치) |
| 2 | PCIe 라이저 1/슬롯 1 |
| 3 | PCIe 라이저 2/슬롯 2 |
| 4 | 전력 공급 장치(최대 2개, 1+1로 이중화). 각 전력 공급 장치에는 전력 공급 장치 결함 LED와 AC 전원 LED가 있습니다.<br>결함 LED가 다음과 같은 경우:<br>• 꺼짐 - 전원 공급 장치가 정상적으로 작동하고 있습니다.<br>• 황색, 깜박임 - 이벤트 경고 임계값에 도달했지만 전원 공급 장치가 계속 작동하고 있습니다.<br>• 황색, 계속 켜져 있음 - 중대한 결함 임계값에 도달하여 전원 공급 장치가 종료되었습니다(예: 팬 작동 중단, 과열 상태).<br>AC 전원 LED가 다음과 같은 경우:<br>• 녹색, 계속 켜져 있음 - AC 전원이 정상이고 DC 출력도 정상입니다.<br>• 녹색, 깜박임 - AC 전원은 정상인데, DC 출력이 활성화되지 않았습니다.<br>• 꺼짐 - 전원 공급 장치에 AC 전원이 연결되지 않았습니다.<br>자세한 내용은 전원 사양을 참조하십시오. |

| **Component(**구성 요소**)** | 설명 |
|---|---|
| 5 | **10Gbps** 클러스터 포트**(**포트 **2, enp10s0,** 네트워크 어댑터 **1)**: 이는 어플라이언스 mLOM 슬롯의 Cisco VIC(Virtual Interface Card) 1227에 있는 두 번째 10Gbps 포트입니다. 후면 패널에서는 이 포트에 포트 **2** 레이블을 지정하고 Maglev 구성 마법사에서는 이를 **enp10s0** 및 네트워크 어댑터 **1**로 식별합니다. 이 포트를 Cisco DNA Center 클러스터의 다른 노드에 대한 연결을 사용하여 스위치에 연결합니다.<br>이 포트에는 링크 상태("ACT") LED와 링크 속도("LINK") LED가 있습니다.<br>링크 상태 LED가 다음과 같은 경우:<br>• 녹색(깜박임) - 활성 링크에 트래픽이 있습니다.<br>• 녹색 - 링크가 활성 상태이지만 트래픽이 없습니다.<br>• 꺼짐 - 링크가 없습니다.<br>링크 속도 LED가 다음과 같은 경우:<br>• 녹색 - 링크 속도가 10Gbps입니다.<br>• 황색 - 링크 속도가 1Gbps입니다.<br>• 꺼짐 - 링크 속도가 100Mbps 이하입니다.<br>참고 엔터프라이즈 및 클러스터 포트는 10Gbps에서만 작동해야 합니다. |

| **Component(**구성 요소**)** | 설명 |
|---|---|
| 6 | **10Gbps** 엔터프라이즈 포트**(**포트 **1, enp9s0,** 네트워크 어댑터 **4)**: 이는 어플라이언스 mLOM 슬롯의 Cisco VIC(Virtual Interface Card) 1227에 있는 첫 번째 10Gbps 포트입니다. 후면 패널에서는 이 포트에 포트 **1** 레이블을 지정하고 Maglev 구성 마법사에서는 이를 **enp9s0** 및 네트워크 어댑터 **4**로 식별합니다. 이 포트를 Cisco DNA Center에서 관리할 네트워킹 장비에 대한 IP 연결성을 사용하는 스위치에 연결합니다.<br>이 포트에는 링크 상태("ACT") LED와 링크 속도("LINK") LED가 있습니다.<br>링크 상태 LED가 다음과 같은 경우:<br>• 녹색(깜박임) - 활성 링크에 트래픽이 있습니다.<br>• 녹색 - 링크가 활성 상태이지만 트래픽이 없습니다.<br>• 꺼짐 - 링크가 없습니다.<br>속도 LED가 다음과 같은 경우:<br>• 녹색 - 링크 속도가 10Gbps입니다.<br>• 황색 - 링크 속도가 1Gbps입니다.<br>• 꺼짐 - 링크 속도가 100Mbps 이하입니다.<br>참고 Cisco DNA Center 어플라이언스 엔터프라이즈 및 클러스터 포트는 10Gbps에서만 작동해야 합니다. |
| 7 | USB 3.0 포트 2개 |

| **Component**(구성 요소) | 설명 |
|---|---|
| 8 | **1Gbps CIMC** 포트**(M)**: 이 포트는 두 USB 포트의 오른쪽에 포함된 포트이며 RJ45 시리얼 포트의 왼쪽에 있습니다. 후면 패널에서는 여기에 **M** 레이블을 지정하고 어플라이언스의 CIMC GUI에 대한 브라우저 액세스를 활성화할 때 IP 주소를 할당합니다(CIMC에 대한 브라우저 액세스 활성화 참조). 이 포트는 Cisco DNA Center 어플라이언스 섀시 및 소프트웨어의 대역 외(OOB) 관리를 위해 예약되어 있습니다. 전용 OOB 엔터프라이즈 관리 네트워크에 대한 액세스를 제공하는 스위치에 연결합니다.<br>이 포트에는 링크 상태 LED와 링크 속도 LED가 있습니다. 링크 상태 LED가 다음과 같은 경우:<br>• 녹색(깜박임) - 활성 링크에 트래픽이 있습니다.<br>• 녹색 - 링크가 활성 상태이지만 트래픽이 없습니다.<br>• 꺼짐 - 링크가 없습니다.<br>속도 LED가 다음과 같은 경우:<br>• 녹색 - 링크 속도가 1Gbps입니다.<br>• 황색 - 링크 속도가 100Mbps입니다.<br>• 꺼짐 - 링크 속도가 10Mbps 이하입니다. |
| 9 | 시리얼 포트(RJ-45 커넥터) |
| 10 | **1Gbps Cisco DNA Center GUI** 포트**(1, enp1s0f0,** 네트워크 어댑터 **2)**: 첫 번째 Intel i350 1Gb 이더넷 컨트롤러 포트입니다. 이 포트는 어플라이언스 마더보드에 포함되어 있습니다. 후면 패널에서는 이 포트에 **1** 레이블을 지정하고 Maglev 구성 마법사에서는 이를 **enp1s0f0** 및 네트워크 어댑터 **2**로 식별합니다. 전용 엔터프라이즈 관리 네트워크에 대한 액세스를 제공하는 스위치에 연결합니다.<br>이 포트에는 링크 상태 LED와 링크 속도 LED가 있습니다. 상태 LED가 다음과 같은 경우:<br>• 녹색(깜박임) - 활성 링크에 트래픽이 있습니다.<br>• 녹색 - 링크가 활성 상태이지만 트래픽이 없습니다.<br>• 꺼짐 - 링크가 없습니다.<br>속도 LED가 다음과 같은 경우:<br>• 녹색 - 링크 속도가 1Gbps입니다.<br>• 황색 - 링크 속도가 100Mbps입니다.<br>• 꺼짐 - 링크 속도가 10Mbps 이하입니다. |

| **Component(**구성 요소**)** | 설명 |
|---|---|
| 11 | **1Gbps** 클라우드 포트**(2, enp1s0f1,** 네트워크 어댑터 **3)**: 이는 두 번째 임베디드 1Gbps 이더넷 컨트롤러 포트입니다. 후면 패널에서는 이 포트에 **2** 레이블을 지정하고 Maglev 구성 마법사에서는 이를 **enp1s0f1** 및 네트워크 어댑터 **3**으로 식별합니다. 이 포트는 선택 사항입니다. 이는 **10Gbps** 엔터프라이즈 포트(포트 1, enp9s0, 네트워크 어댑터 4)를 통해 인터넷에 연결할 수 없는 경우에 사용됩니다.<br>이 포트에는 링크 상태 LED와 링크 속도 LED가 있습니다. 링크 상태 LED가 다음과 같은 경우:<br>• 녹색(깜박임) - 활성 링크에 트래픽이 있습니다.<br>• 녹색 - 링크가 활성 상태이지만 트래픽이 없습니다.<br>• 꺼짐 - 링크가 없습니다.<br>속도 LED가 다음과 같은 경우:<br>• 녹색 - 링크 속도가 1Gbps입니다.<br>• 황색 - 링크 속도가 100Mbps입니다.<br>• 꺼짐 - 링크 속도가 10Mbps 이하입니다. |
| 12 | VGA 비디오 포트(DB-15). 이 포트 주변의 이 패널 영역은 파란색입니다. |
| 13 | 파란색 LED 로케이터 버튼 |

# 제품 외장 사양

다음 표에는 어플라이언스의 물리적 사양이 나와 있습니다.

표 ***2:*** 제품 외장 사양

| 설명 | 사양 |
|---|---|
| 높이 | 1.7인치(4.32cm) |
| 너비 | 16.89인치(43.0cm)<br>핸들 포함:<br>18.98인치(48.2cm) |
| 깊이(길이) | 29.8인치(75.6cm)<br>핸들 포함:<br>30.98인치(78.7cm) |

| 설명 | 사양 |
| --- | --- |
| 전면 여유 공간 | 3인치(76mm) |
| 측면 여유 공간 | 1인치(25mm) |
| 후면 여유 공간 | 6인치(152mm) |
| 최대 무게(완전 로드된 섀시) | 37.9파운드(17.2kg) |

# 환경 사양

다음 표에는 어플라이언스의 환경 사양이 나와 있습니다.

표 ***3:*** 환경 사양

| 설명 | 사양 |
| --- | --- |
| 작동 온도 | 5~35°C(41~95°F)<br>해발 고도 1000피트(305m)마다 최대 온도가 1°C씩 감소합니다. |
| 온도, 비작동(어플라이언스 보관 또는 운송 시) | −40~65°C(−40~149°F) |
| 작동 습도 | 28°C(82°F)에서 10%~90%, 비응결 |
| 습도, 비작동 | 28°C(82°F)에서 5%~93% |
| 작동 고도 | 0~10,000피트(0~3,000m) |
| 고도, 비작동(어플라이언스 보관 또는 운송 시) | 0~40,000피트(0~12,192m) |
| 음향 출력 레벨, A 가중 측정, ISO7779 LwAd(벨), 23°C(73°F)에서 작동 시 | 5.4 |
| 음압 레벨, A 가중 측정, ISO7779 LpAm(dBA), 23°C(73°F)에서 작동 시 | 37 |

# 전원 사양

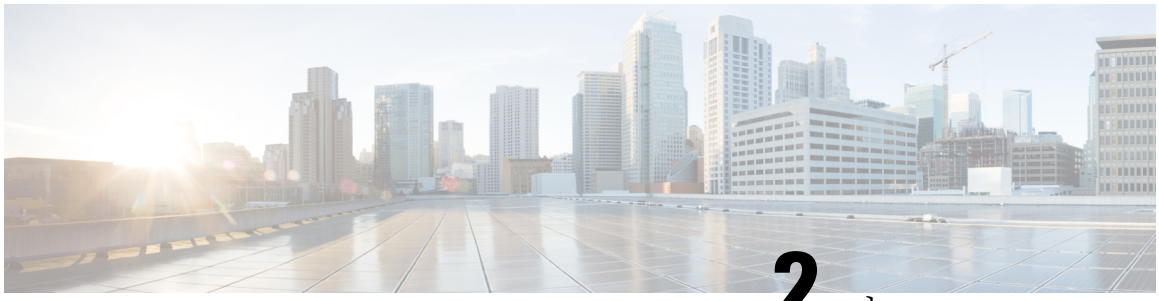
어플라이언스와 함께 제공되는 듀얼 770W AC 전력 공급 장치(Cisco 부품 번호 UCSC-PSU1-770W)에 대한 사양이 아래 표에 나와 있습니다.

주의 어플라이언스에서 여러 전원 공급 장치 유형을 혼합 사용하지 마십시오. 두 전원 공급 장치가 동일해야 합니다.

표 ***4: AC*** 전원 공급 장치 사양

| 설명 | 사양 |
|---|---|
| AC 입력 전압 | 공칭 범위: 100–120VAC, 200–240VAC<br>(범위: 90-132VAC, 180-264VAC) |
| AC 입력 주파수 | 공칭 범위: 50~60Hz<br>(범위: 47–63Hz) |
| 최대 AC 입력 전류 | 9.5A(100VAC)<br>4.5A(208VAC) |
| 최대 입력 볼트암페어 | 950VA(100VAC) |
| PSU당 최대 출력 전원 | 770W |
| 최대 돌입 전류 | 15A(하위 주기 기간) |
| 최대 유지 시간 | 12ms(770W) |
| 전력 공급 장치 출력 전압 | 12VDC |
| 전원 공급 장치 대기 전압 | 12VDC |
| 효율성 등급 | Climate Savers 플래티넘 효율성(80Plus Platinum 인증) |
| 폼 팩터 | RSP2 |
| 입력 커넥터 | IEC320 C14 |

Cisco UCS Power Calculator(http://ucspowercalc.cisco.com)를 사용하면 정확한 어플라이언스 구성에 대한 구체적인 전력 정보를 얻을 수 있습니다.



2 장

# 구축 계획


- 워크플로 계획, 13 페이지
- Cisco DNA Center 및 소프트웨어 정의 액세스 정보, 14 페이지
- 인터페이스 케이블 연결, 15 페이지
- 필수 서브넷 및 추가 IP 주소, 17 페이지
- 필수 인터넷 URL 및 FQDN(Fully Qualified Domain Name), 21 페이지
- 인터넷에 대한 보안 액세스 제공, 23 페이지
- 필수 네트워크 포트, 24 페이지
- 필수 SD-Access 포트 및 프로토콜, 26 페이지
- 필수 구성 정보, 34 페이지
- 필수 초기 설정 정보, 36 페이지


## 워크플로 계획

다음 표에는 어플라이언스 설치, 구성 및 설정을 시도하기 전에 수행해야 하는 계획 및 정보 수집 작업에 대해 자세히 설명되어 있습니다. 이 표의 작업을 완료하면 데이터 센터에 어플라이언스를 물리적으로 설치하여 계속 진행할 수 있습니다.

Cisco DNA Center의 개요와 설치 및 구성 프로세스에 대한 개요를 제공하는 비디오 시리즈를 보려면 이 링크를 클릭하십시오.

자세한 내용은 Cisco DNA Center 및 소프트웨어 정의 액세스 정보를 참조하십시오.

표 *5:* 작업 계획

| 단계 | 설명 |
|---|---|
| 1 | 독립형 및 클러스터 설치를 위해 권장되는 케이블 연결 및 스위칭 요건 검토: 인터페이스 케이블 연결 |
| 2 | 어플라이언스 구성 시 적용할 IP 주소 지정, 서브넷 지정 및 기타 IP 트래픽 정보 수집: 필수 서브넷 및 추가 IP 주소 |
| 3 | 웹 기반 리소스에 대한 필수 액세스를 위한 솔루션 준비: 필수 인터넷 URL 및 FQDN(Fully Qualified Domain Name), 인터넷에 대한 보안 액세스 제공 |

| 단계 | 설명 |
|---|---|
| 4 | Cisco DNA Center 트래픽에 대한 방화벽 및 보안 정책 재구성: 필수 네트워크 포트. Cisco DNA Center를 사용하여 SDA 네트워크를 관리하는 경우, 필수 SD-Access 포트 및 프로토콜도 참조하십시오. |
| 5 | 어플라이언스 구성 및 최초 설정 시 사용된 추가 정보 수집: 필수 구성 정보 및 필수 초기 설정 정보 |

# Cisco DNA Center 및 소프트웨어 정의 액세스 정보

Cisco의 소프트웨어 정의 액세스 패브릭 아키텍처(SD-Access 또는 SDA라고도 함)를 사용하는 네트워크 등 모든 유형의 네트워크를 관리하는 데 Cisco DNA Center를 사용할 수 있습니다. 혁신적인 SDA 접근 방식은 기존 네트워크를 의도 기반 네트워크로 변환하며, 이때 비즈니스 논리가 네트워크의 물리적인 부분이 되므로 구성, 프로비저닝, 트러블슈팅 등 일상적인 작업을 쉽게 자동화할 수 있습니다. Cisco SD-Access 솔루션을 사용하면 네트워크를 비즈니스 요구 사항에 맞게 조정하고 문제 해결을 개선하며 보안 침해가 미치는 영향을 감소하는 데 걸리는 시간을 줄일 수 있습니다.

SDA 솔루션에 대한 완전한 논의 내용은 이 가이드에 나와 있지 않습니다. Cisco DNA Center에서 사용하기 위해 SDA 패브릭 아키텍처를 구현할 계획을 수립하는 네트워크 설계자 및 관리자는 다음 리소스에서 추가 정보 및 지침을 찾을 수 있습니다.

- SDA 및 Cisco Digital Network Architecture에 대한 간략한 소개는 백서인 Cisco Digital Network Architecture 비전 - 개요를 참조하십시오.
- Cisco DNA Center에서 SD-Access를 활용하여 일반 네트워킹 접근 방식 및 기술로는 불가능한 솔루션을 자동화하는 방법에 대한 자세한 내용은 소프트웨어 정의 액세스: 의도 기반 네트워킹 활성화를 참조하십시오.
- 네트워크에서 SDA를 구현하는 방법을 시연하는 검증된 설계는 Cisco 소프트웨어 정의 액세스 설계 가이드의 최신 버전을 참조하십시오.
- SDA 액세스 세분화를 사용하여 네트워크 보안을 개선하는 방법에 대한 지침은 소프트웨어 정의 액세스 세분화 설계 가이드를 참조하십시오.
- 무선 관련 설계 지침에 대해서는 SD-Access 무선 설계 및 구축 가이드를 참조하십시오.
- Cisco DNA Center를 사용하여 SDA를 구축하는 방법에 대한 지침은 소프트웨어 정의 액세스 구축 가이드를 참조하십시오.
- Cisco DNA Center 및 SDA 솔루션의 기초인 Digital Network Architecture와 이 혁신적인 아키텍처에서 기타 Cisco 및 타사 제품/솔루션이 수행하는 역할에 대한 자세한 내용은 Cisco DNA Design Zone을 참조하십시오.
- 기타 설계 가이드, 구축 가이드 및 백서는 Cisco Design Zone을 참조하십시오.

# 인터페이스 케이블 연결

어플라이언스의 포트를 다음 유형의 네트워크 액세스를 제공하는 스위치에 연결합니다. 최소한 Cisco DNA Center 기능에 필요하므로 엔터프라이즈 및 클러스터 포트 인터페이스를 구성해야 합니다.

- **(**필수**) 10Gbps** 클러스터 포트**(**포트 **2, enp10so,** 네트워크 어댑터 **1)**: 어플라이언스 mLOM 슬롯의 VIC 1227 카드에 있는 왼쪽 포트입니다. 이 포트는 Cisco DNA Center 클러스터에서 마스터 및 추가 기능 노드 간의 통신을 활성화하는 데 사용됩니다. 이 포트를 클러스터의 다른 노드에 연결하는 스위치에 케이블로 연결하고 포트에 대한 서브넷 마스크를 사용하여 한 개의 IP 주소를 구성하십시오.

  구성 시 인터페이스에 클러스터 링크 옵션을 할당할 때까지는 Maglev 구성 마법사로 인해 작업을 진행할 수 없습니다. 포트 enp10so를 클러스터 링크로 지정하는 것이 좋습니다. 그러나 구성이 완료된 후에는 클러스터 링크로 표시된 인터페이스를 변경할 수 없다는 점에 유의해야 합니다. 나중에 클러스터 링크로 표시된 인터페이스를 변경해야 하는 경우에는 재설치를 수행해야 합니다. 이를 염두에 두고 클러스터 포트를 IP 주소로 설정하는 것이 좋습니다. 따라서 향후 3개의 노드로 이루어진 클러스터로 확장하는 작업이 가능합니다. 또한 클러스터 링크 인터페이스가 스위치 포트에 연결되어 있고 UP(작동) 상태인지 확인합니다.

- **(**선택 사항**) 1Gbps Cisco DNA Center GUI** 포트**(1, enp1s0f0,** 네트워크 어댑터 **2)**: 이 포트를 사용하면 Cisco DNA Center 그래픽 유저 인터페이스에 액세스할 수 있습니다. 이 포트는 사용자가 어플라이언스에서 소프트웨어를 사용할 수 있도록 지원하기 위해 사용됩니다. 이 포트를 엔터프라이즈 관리 네트워크에 연결하는 스위치에 케이블로 연결하고 포트에 대한 서브넷 마스크를 사용하여 한 개의 IP 주소를 구성하십시오.

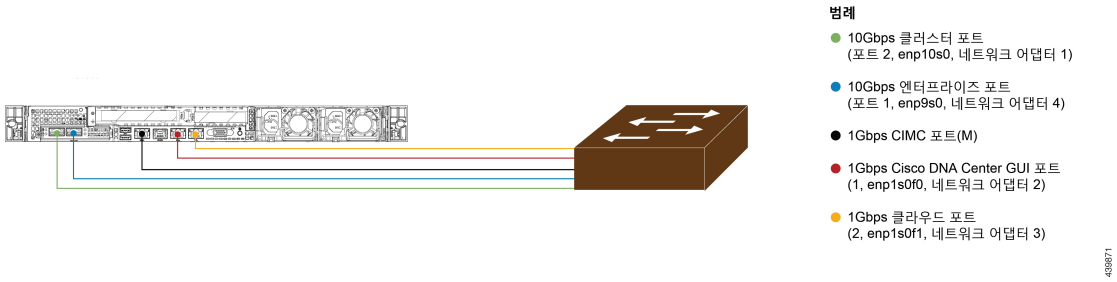
- **(**선택 사항**) 1Gbps** 클라우드 포트**(2, enp1s0f1,** 네트워크 어댑터 **3)**: 이 포트는 선택 사항입니다. 10Gbps 엔터프라이즈 포트(포트 1, enp9s0, 네트워크 어댑터 4)를 사용하여 어플라이언스를 인터넷(인터넷 프록시 서버 포함)에 연결할 수 없는 경우에만 사용합니다. 클라우드 포트를 사용해야 하는 경우, 이 포트를 인터넷 프록시 서버에 연결하는 스위치에 케이블로 연결하고 포트에 대한 서브넷 마스크를 사용하여 한 개의 IP 주소를 구성하십시오.

- **(**필수**) 10Gbps** 엔터프라이즈 포트**(**포트 **1, enp9s0,** 네트워크 어댑터 **4)**: 이는 어플라이언스 mLOM 슬롯에 있는 VIC 1227 카드의 오른쪽 포트입니다. 이 포트는 Cisco DNA Center에서 네트워크와 통신하고 네트워크를 관리할 수 있도록 지원하기 위해 사용됩니다. 이 포트를 엔터프라이즈 네트워크에 연결하는 스위치에 케이블로 연결하고 포트에 대한 서브넷 마스크를 사용하여 한 개의 IP 주소를 구성하십시오.

- **(**선택 사항이지만 권장됨**) 1Gbps CIMC** 포트**(M)**: 이 포트를 사용하면 CIMC 대역 외 어플라이언스 관리 인터페이스 및 해당 그래픽 유저 인터페이스에 대한 브라우저 액세스가 가능해집니다. 이 포트는 어플라이언스 및 해당 하드웨어를 관리할 수 있도록 지원하는 데 사용됩니다. 이 포트를 엔터프라이즈 관리 네트워크에 연결하는 스위치에 케이블로 연결하고 포트에 대한 서브넷 마스크를 사용하여 한 개의 IP 주소를 구성하십시오.

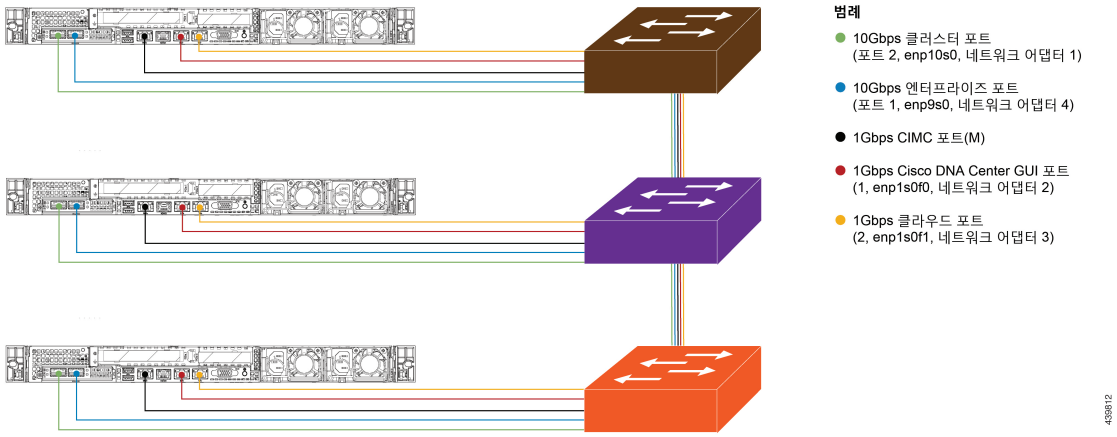
다음 그림에는 단일 노드 Cisco DNA Center 클러스터에 대해 권장되는 연결이 나와 있습니다.

그림 *3:* 단일 노드 클러스터에 대한 케이블 연결 권장 사항




다음 그림에는 3개의 노드로 이루어진 Cisco DNA Center 클러스터에 대해 권장되는 연결이 나와 있습니다. 3개의 노드로 이루어진 클러스터의 각 노드에 대한 연결 중 하나 외에는 모두 단일 노드 클러스터에 대한 연결 중과 동일하며 동일한 포트를 사용합니다. 예외 사항은 클러스터 포트(포트 2, enp10so, 네트워크 어댑터 1)이며, 이는 3개의 노드로 이루어진 클러스터의 각 호스트에서 다른 호스트와 통신할 수 있도록 하는 데 필요합니다.

그림 *4: 3*개의 노드로 이루어진 클러스터에 대한 케이블 연결 권장 사항




후면 패널 포트와 해당 포트가 사용되는 방법에 대한 간단한 비디오 프리젠테이션을 보려면 어슈어런스 및 SD-Access를 위한 Cisco DNA Center 어플라이언스 꺼내기("시작하기" 섹션 아래)의 처음 5분간의 내용을 참조하십시오.

각 포트에 대한 자세한 내용은 전면 패널 및 후면 패널의 Cisco UCS C220 M4 섀시에 대해 함께 제공되는 설명 및 후면 패널 다이어그램을 참조하십시오.

참고 다중 노드 클러스터 구축 시에는 모든 멤버 노드가 동일한 네트워크와 동일한 사이트에 있어야 합니다. 어플라이언스에서는 여러 네트워크 또는 사이트 전체에 걸친 노드 배포를 지원하지 않습니다.

10Gbps 엔터프라이즈 및 클러스터 포트에 케이블로 연결하는 경우, 두 포트 모두 다음의 미디어 유형만 지원한다는 점에 유의하십시오.

- FP-10G-USR(매우 짧은 범위, MMF)
- SFP-10G-SR(짧은 범위, MMF)

- SFP-10G-LR(긴 범위, SMF)
- 10GBASE-CU SFP+ Cable 1m
- 10GBASE-CU SFP+ Cable 3m
- 10GBASE-CU SFP+ Cable 5m
- 10GBASE-CU SFP+ 케이블 7m
- SFP-10GB-ACU 케이블 7m

# 필수 서브넷 및 추가 **IP** 주소

설치를 시작하기 전에 네트워크에 사용하려는 각 어플라이언스 포트에 할당할 수 있는 충분한 IP 주소가 있는지 확인해야 합니다. 어플라이언스를 단일 노드 클러스터로 설치하는지 아니면 3개의 노드로 이루어진 클러스터의 마스터 또는 추가 기능 노드로 설치하는지에 따라 다음과 같은 NIC(어플라이언스 포트) 주소가 필요합니다.

- 엔터프라이즈 포트 주소**(**필수**)**: 서브넷 마스크가 있는 IP 주소 1개
- 클러스터 포트 주소**(**필수**)**: 서브넷 마스크가 있는 IP 주소 1개
- 관리 포트 주소**(**선택 사항**)**: 서브넷 마스크가 있는 IP 주소 1개
- 클라우드 포트 주소**(**선택 사항**)**: 서브넷 마스크가 있는 IP 주소 1개. 이 포트는 선택 사항이며, 엔터프라이즈 포트를 사용하여 클라우드에 연결할 수 없는 경우에만 사용됩니다. 포트를 이 용도로 사용해야 하는 경우가 아니면 클라우드 포트에 대한 IP 주소는 필요하지 않습니다.
- **CIMC** 포트 주소**(**선택 사항이지만 권장됨**)**: 서브넷 마스크가 있는 IP 주소 1개

참고 이러한 요건을 위해 호출되는 모든 IP 주소는 유효한 IPv4 넷마스크를 사용하는 유효한 물리적 IPv4 주소여야 합니다. 주소와 해당 서브넷이 겹치지 않는지 확인합니다. 주소와 해당 서브넷이 겹치는 경우 서비스 통신 문제가 발생할 수 있습니다.

또한 다음과 같은 추가 IP 주소 및 전용 IP 서브넷이 필요합니다. 어플라이언스를 구성할 때 이에 대한 프롬프트가 표시되고 해당 항목이 적용됩니다.

1. 클러스터 가상 **IP** 주소: 클러스터당 구성된 네트워크 인터페이스당 1개의 VIP(가상 IP) 주소입니다. 이 요건은 향후 3개의 노드로 이루어진 클러스터로 변환될 가능성이 높은 단일 노드 클러스터 및 3개의 노드로 이루어진 클러스터에 적용됩니다. 구성하는 각 네트워크 인터페이스에 대한 VIP를 제공해야 합니다. 각 VIP는 구성된 해당 인터페이스의 IP 주소와 동일한 서브넷에 있어야 합니다. 각 어플라이언스에는 엔터프라이즈, 클러스터, 관리 및 클라우드라는 네 가지 인터페이스가 있습니다. 최소한 엔터프라이즈 및 클러스터 포트 인터페이스는 구성해야 합니다. Cisco DNA Center 기능에 필요하기 때문입니다. 인터페이스는 서브넷 마스크 및 하나 이상의 연결된 게이트웨이 또는 정적 경로와 함께 해당 인터페이스에 대한 IP를 제공하는 경우 구성된 것으로 간주됩

니다. 구성 시 인터페이스를 완전히 건너뛰면 해당 인터페이스는 구성되지 않은 것으로 간주됩니다.

다음에 유의하십시오.

- 단일 노드 설정이 있고 나중에 이를 3개의 노드로 이루어진 클러스터로 변환할 계획이 없는 경우에는 가상 IP 주소를 지정할 필요가 없습니다. 그러나 변환 계획이 있는 경우에는 구성된 모든 네트워크 인터페이스에 대해 가상 IP 주소를 지정해야 합니다(3개의 노드로 이루어진 클러스터의 경우와 마찬가지).
- 단일 노드 클러스터에 대한 내부 클러스터 연결이 가동 중지되면 관리 및 엔터프라이즈 인터페이스와 연결된 가상 IP 주소도 가동 중지됩니다. 이렇게 되면 클러스터 내부 링크가 복원될 때까지(SWIM 및 ISE 통합이 작동하지 않으며 NDP 컬렉터에서 정보를 수집할 수 없기 때문에 어슈어런스 데이터가 표시되지 않음) Cisco DNA Center를 사용할 수 없습니다.

2. 기본 게이트웨이 **IP** 주소: 네트워크의 기본 설정된 게이트웨이에 대한 IP 주소입니다. 트래픽과 매치하는 다른 경로가 없을 경우 이 IP 주소를 통해 트래픽이 라우팅됩니다. 일반적으로는 인터넷에 액세스하는 네트워크 구성의 인터페이스에 기본 게이트웨이를 할당해야 합니다. Cisco DNA Center 구축 시 주의해야 하는 보안 고려 사항에 대한 내용은 Cisco Digital Network Architecture Center 보안 모범 사례 가이드를 참조하십시오.

3. **DNS** 서버 **IP** 주소: 하나 이상의 네트워크 기본 설정 DNS 서버에 대한 IP 주소입니다. 구성 시 여러 DNS 서버 IP 주소와 넷마스크를 공백으로 구분된 목록으로 입력하여 지정할 수 있습니다.

4. **(**선택 사항**)** 정적 경로 주소: 하나 이상의 정적 경로에 대한 IP 주소, 서브넷 마스크 및 게이트웨이입니다. 구성 시 여러 정적 경로 IP 주소, 넷마스크 및 게이트웨이를 공백으로 구분된 목록으로 입력하여 지정할 수 있습니다.

   어플라이언스의 모든 인터페이스에 대해 하나 이상의 정적 경로를 설정할 수 있습니다. 기본 게이트웨이 이외의 특정 방향으로 트래픽을 라우팅하려면 정적 경로를 제공해야 합니다. 정적 경로가 포함된 각 인터페이스는 IP 경로 명령 표에서 트래픽이 라우팅되는 디바이스로 설정됩니다. 따라서 트래픽이 전송되는 인터페이스와 정적 경로의 방향을 일치시키는 것이 중요합니다.

   스위치 및 라우터에서 사용하는 것과 같은 네트워크 디바이스 라우팅 표에서는 정적 경로를 사용하지 않는 것이 좋습니다. 동적 라우팅 프로토콜은 이 경우에 더 적합합니다. 그러나 다른 방식으로도 연결할 수 없는 네트워크의 특정 부분에 대한 어플라이언스 액세스를 허용해야 하는 경우에는 이를 추가해야 합니다.

5. **NTP** 서버 **IP** 주소: 하나 이상의 NTP(Network Time Protocol) 서버에 대한 DNS 확인 가능 호스트 이름 또는 IP 주소입니다.

   구성 시 여러 NTP 서버 IP/넷마스크 또는 호스트 이름을 공백으로 구분된 목록으로 입력하여 지정할 수 있습니다. 프로덕션 구축의 경우 최소 3개의 NTP 서버를 구성하는 것이 좋습니다.

   이러한 서버는 사전 검사된 하드웨어 동기화 중에 지정하게 되며, 클러스터의 각 어플라이언스에서 소프트웨어를 구성할 때 다시 지정하게 됩니다. 시간 동기화는 다중 호스트 클러스터 전체에서 데이터 정확도와 처리를 조정하는 데 있어 매우 중요합니다. 어플라이언스를 프로덕션에서 구축하기 전에 어플라이언스 시스템 시계의 시간이 최신 상태이고 지정한 NTP(Network Time Protocol) 서버가 정확한 시간을 유지하고 있는지 확인합니다. Cisco ISE(Identity Services Engine)와 어플라

이언스를 통합하려는 경우에는 또한 ISE가 어플라이언스와 동일한 NTP 서버와 동기화되도록 해야 합니다.

6. 서비스 서브넷: 어슈어런스, 인벤토리 수집 등의 내부 애플리케이션 서비스 간의 통신을 위해 IP를 관리하고 얻는 데 사용할 어플라이언스의 전용 IP 서브넷 1개를 식별합니다. 전용 IPv4 서비스 서브넷은 Cisco DNA Center의 내부 네트워크 또는 외부 네트워크에서 사용되는 다른 서브넷과 충돌하거나 중복되지 않아야 합니다. 서브넷의 최소 크기는 21비트입니다. IPv4 서비스 서브넷은 다음 주소 범위를 지원하는 프라이빗 네트워크에 대해 IETF RFC 1918 및 RFC 6598 사양을 준수해야 합니다.

   - 10.0.0.0/8
   - 172.16.0.0/12
   - 192.168.0.0/16
   - 100.64.0.0/10

   자세한 내용은 RFC 1918, 프라이빗 인터넷에 대한 주소 할당 및 RFC 6598, IANA-공유 어드레스 스페이스용 예약 IPv4 접두사를 참조하십시오.

중요

- 유효한 CIDR 서브넷을 지정했는지 확인합니다. 그렇지 않으면 잘못된 비트가 172.17.1.0/20 및 172.17.61.0/20 서브넷에 표시됩니다.
- Cisco DNA Center 어플라이언스의 구성이 완료된 후에는 어플라이언스를 먼저 이미지로 다시 설치하지 않고는 다른 서브넷을 할당할 수 없습니다(자세한 내용은 "어플라이언스 구성" 장의 "어플라이언스를 이미지로 다시 설치" 항목 참조).

7. 클러스터 서비스 서브넷: 데이터베이스 액세스, 메시지 버스 등의 인프라 서비스 간의 통신을 위해 IP를 관리하고 얻는 데 사용할 어플라이언스의 전용 IP 서브넷 1개를 식별합니다. 전용 IPv4 클러스터 서비스 서브넷은 Cisco DNA Center의 내부 네트워크 또는 외부 네트워크에서 사용되는 다른 서브넷과 충돌하거나 중복되지 않아야 합니다. 서브넷의 최소 크기는 21비트입니다. IPv4 클러스터 서비스 서브넷은 다음 주소 범위를 지원하는 프라이빗 네트워크에 대해 IETF RFC 1918 및 RFC 6598 사양을 준수해야 합니다.

   - 10.0.0.0/8
   - 172.16.0.0/12
   - 192.168.0.0/16
   - 100.64.0.0/10

   자세한 내용은 RFC 1918, 개인 인터넷에 대한 주소 할당 및 RFC 6598, IANA-공유 어드레스 스페이스용 예약 IPv4 접두사를 참조하십시오.

   10.10.10.0/21을 서비스 서브넷으로 지정하려는 경우, 이러한 두 서브넷이 중복되지 않으므로 10.0.8.0/21의 클러스터 서비스 서브넷을 지정할 수도 있습니다. 또한 구성 마법사에서는 이러한 서브넷 간에 중복 항목(있는 경우)을 탐지하고 중복을 수정하라는 프롬프트를 표시합니다.

중요

- 유효한 CIDR 서브넷을 지정했는지 확인합니다. 그렇지 않으면 잘못된 비트가 172.17.1.0/20 및 172.17.61.0/20 서브넷에 표시됩니다.
- Cisco DNA Center 어플라이언스의 구성이 완료된 후에는 어플라이언스를 먼저 이미지 재설치하지 않고 다른 서브넷을 할당할 수 없습니다(자세한 내용은 "어플라이언스 구성" 장의 "어플라이언스이미지 재설치" 항목 참조).

2개의 서비스 및 클러스터 서비스 서브넷에 권장되는 총 IP 어드레스 스페이스에는 4,096개의 주소가 포함되어 있으며, 각각 2,048개의 주소로 구성된 2개의 /21 서브넷으로 분류됩니다. 2개의 /21 서브넷은 중복되지 않아야 합니다. Cisco DNA Center의 내부 서비스는 작동하기 위해 전용 IP 주소 집합이 필요합니다(Cisco DNA Center 마이크로 서비스 아키텍처의 요건). 이 요건을 충족하려면 Cisco DNA Center 시스템당 두 개의 전용 서브넷을 할당해야 합니다.

어플라이언스에서 이만큼의 어드레스 스페이스를 필요로 하는 한 가지 이유는 시스템 성능을 유지하기 위함입니다. 여기서는 동-서(노드 간) 통신을 위해 내부 라우팅 및 터널링 기술이 사용되므로 중복되는 어드레스 스페이스를 사용하면 어플라이언스에서 내부적으로 가상 라우팅 및 포워딩 FIB를 실행해야 합니다. 이렇게 하면 한 서비스에서 다른 서비스로 이동하는 패킷에 대해 여러 encaps/decap가 전송되며, 상위 계층에서 연계된 영향을 줄 수 있는 매우 낮은 레벨의 높은 내부 레이턴시가 발생합니다.

또 다른 이유는 Cisco DNA Center Kubernetes 기반 서비스 컨테이너화 아키텍처입니다. 각 어플라이언스에서는 Kubernetes K8 노드별로 이 공간에 있는 IP 주소를 사용합니다. 여러 노드가 단일 서비스를 구성할 수 있습니다. 현재 Cisco DNA Center에서는 100개가 넘는 서비스를 지원하며, 각 서비스에는 항상 여러 개의 IP 주소와 새로운 기능 및 해당하는 서비스가 추가되어야 합니다. 어드레스 스페이스 요건은 Cisco에서 IP가 부족해지거나 고객이 단순히 시스템을 업그레이드하기 위해 연속된 어드레스 스페이스를 재할당해야 하는 일 없이 새로운 서비스와 기능을 추가할 수 있도록 처음부터 크게 유지됩니다.

이러한 서브넷을 통해 지원되는 서비스는 Layer 3에서도 활성화됩니다. 특히 클러스터 서비스 공간은 애플리케이션 및 인프라 서비스 간에 데이터를 전달하며 많이 사용됩니다.

RFC 1918 및 RFC 6598 요건은 클라우드에서 패키지 및 업데이트를 다운로드하기 위한 Cisco DNA Center의 요건 때문입니다. 선택한 IP 범위가 RFC 1918 및 RFC 6598과 일치하지 않을 경우, 이는 공용 IP 중복 문제로 빠르게 이어질 수 있습니다.

# 인터페이스 이름 및 마법사 구성 순서

다음 표에 나와 있는 것처럼, 인터페이스 이름 및 이러한 인터페이스가 Maglev 구성 마법사에서 구성되는 순서는 Cisco DNA Center 어플라이언스의 M4 및 M5 새시 모델에 따라 달라집니다.

표 *6:* 인터페이스 이름 및 마법사 구성 순서

| 기능 | **Cisco DNA Center** 어플라이언스 섀시 모델 | **Interface Name** | **Maglev** 구성 마법사에서의 구성 순서 |
|---|---|---|---|
| **Cluster(**클러스터**)**: 클러스터 노드에 어플라이언스를 연결합니다. | **M4** | **enp10s0** | 네트워크 어댑터 **#1** |
| | M5 | enp94s0f1 | 네트워크 어댑터 #4 |
| **Management(**관리**)**: 관리 네트워크에서 Cisco DNA Center GUI에 액세스할 수 있습니다. | **M4** | **enp1s0f0** | 네트워크 어댑터 **#2** |
| | M5 | eno1 | 네트워크 어댑터 #1 |
| **Cloud(**클라우드**)**: 다른 인터페이스를 이 목적으로 사용할 수 없는 경우 인터넷 액세스를 제공합니다. | **M4** | **enp1s0f1** | 네트워크 어댑터 **#3** |
| | M5 | eno2 | 네트워크 어댑터 #2 |
| **Enterprise(**엔터프라이즈**)**: 어플라이언스를 엔터프라이즈 네트워크에 연결합니다. | **M4** | **enp9s0** | 네트워크 어댑터 **#4** |
| | M5 | enp94s0f0 | 네트워크 어댑터 #3 |

# 필수 인터넷 URL 및 FQDN(Fully Qualified Domain Name)

어플라이언스를 사용하려면 다음의 URL 및 FQDN(Fully Qualified Domain Name) 표에 대한 보안 액세스가 필요합니다.

이 표에는 각 URL 및 FQDN을 사용하는 기능에 대한 설명이 나와 있습니다. IP 트래픽이 어플라이언스 및 이러한 리소스로 이동할 수 있도록 네트워크 방화벽 또는 프록시 서버 중 하나를 구성해야 합니다. 나열된 URL 및 FQDN에 대해 이 액세스를 제공할 수 없는 경우에는 관련된 기능이 손상되거나 작동하지 않습니다.

인터넷에 대한 프록시 액세스를 위한 요건에 대한 자세한 내용은 인터넷에 대한 보안 액세스 제공을 참조하십시오.

표 7: 필수 URL 및 FQDN 액세스

| 수행할 작업... | ...Cisco DNA Center에서 액세스해야 하는 URL 및 FQDN |
|---|---|
| 시스템 및 애플리케이션 패키지 소프트웨어에 대한 업데이트를 다운로드하고 제품 팀에 사용자 피드백을 제출 | 권장 사항: *.ciscoconnectdna.com:443[1]<br>와일드카드를 사용하지 않으려는 고객은 대신 다음과 같은 URL을 지정할 수 있습니다.<br>• https://www.ciscoconnectdna.com<br>• https://cdn.ciscoconnectdna.com<br>• https://registry.ciscoconnectdna.com<br>• https://registry-cdn.ciscoconnectdna.com |
| Cisco DNA Center 업데이트 패키지 | https://*.ciscoconnectdna.com/*<br>https://*.cloudfront.net/<br>https://maglev-catalog-1.s3.amazonaws.com<br>https://maglev-catalogstaging.s3.amazonaws.com |
| 스마트 어카운트 및 SWIM 소프트웨어 다운로드 | https://apx.cisco.com<br>https://cloudsso.cisco.com/as/token.oauth2<br>https://*.cisco.com/* |
| 사용자 피드백 | https://dnacenter.uservoice.com |
| Cisco Meraki와 통합 | 권장 사항: *.meraki.com:443<br>와일드카드를 사용하지 않으려는 고객은 대신 이러한 URL을 지정할 수 있습니다.<br>• dashboard.meraki.com:443<br>• api.meraki.com:443<br>• n63.meraki.com:443 |

| 수행할 작업... | ...Cisco DNA Center에서 액세스해야 하는 URL 및 FQDN |
|---|---|
| Cisco.com 및 Cisco Smart Licensing과 통합 | *. cisco.com:443<br>와일드카드를 사용하지 않으려는 고객은 대신 이러한 URL을 지정할 수 있습니다.<br>• software.cisco.com<br>• cloudsso.cisco.com<br>• cloudsso1.cisco.com<br>• cloudsso2.cisco.com<br>• apiconsole.cisco.com<br>• api.cisco.com<br>• apx.cisco.com<br>• sso.cisco.com<br>• apmx-prod1-vip.cisco.com<br>• apmx-prod2-vip.cisco.com |
| 사이트 및 위치 맵에서 정확한 정보를 렌더링 | • www.mapbox.com<br>• *.tiles.mapbox.com/* :443. 프록시의 경우, 대상은 *.tiles.mapbox.com/*입니다. |

[1] Cisco에서는 ciscoconnectdna.com 및 해당 하위 도메인을 소유하고 유지 관리합니다. Cisco Connect DNA 인프라에서는 Cisco 보안 및 신뢰 지침을 충족하며, 지속적인 보안 테스트를 실행합니다. 이 인프라는 기본적으로 제공되는 로드 밸런싱 및 자동화 기능을 통해 강력한 성능을 제공하며, 연중무휴 가용성을 보장하기 위해 클라우드 운영 팀에 의해 모니터링 및 유지 관리됩니다.

# 인터넷에 대한 보안 액세스 제공

기본적으로 어플라이언스는 소프트웨어 업데이트, 라이선스 및 디바이스 소프트웨어를 다운로드하고 최신 맵 정보, 사용자 피드백 등을 제공하기 위해 인터넷을 통해 Cisco.com 및 기타 URL에 액세스하도록 구성되어 있습니다.

이러한 목적을 위해 인터넷 연결을 제공하는 것은 필수 요건입니다.

HTTPS 프록시 서버를 사용하는 것은 원격 URL에 안전하게 액세스하기 위해 신뢰할 수 있는 방법입니다. HTTPS 프록시 서버를 사용하여 필수 인터넷 URL 및 FQDN(Fully Qualified Domain Name)에 나열된 URL에 필요한 액세스 권한을 어플라이언스에 제공하는 것이 좋습니다. 설치 시 이 목적으로 사용할 프록시 서버의 URL 및 포트 번호를 프록시의 로그인 크리덴셜과 함께(프록시에서 요구하는 경우) 입력하라는 프롬프트가 표시됩니다.

어플라이언스의 이 릴리스부터는 HTTP를 통한 프록시 서버와의 통신을 지원합니다. 네트워크 내의 어느 곳에서나 HTTPS 프록시 서버를 찾을 수 있습니다. 프록시 서버에서는 HTTPS를 사용하여 인터넷과 통신할 수 있는 반면, 어플라이언스에서는 HTTP를 통해 프록시 서버와 통신합니다. 이러한 이유로 구성 시 프록시를 구성할 때 프록시의 HTTP 포트를 지정해야 할 수 있습니다.

어떤 이유로든 구성 후 프록시 설정을 변경해야 하는 경우 GUI 인터페이스를 통해 이 작업을 수행할 수 있습니다.

# 필수 네트워크 포트

다음 표에는 어플라이언스에서 사용하는 잘 알려진 네트워크 서비스 포트가 나열되어 있습니다. 방화벽 설정을 통해 열든, 아니면 프록시 게이트웨이를 통해 열든 상관없이 어플라이언스에서 오고가는 트래픽에 대해 이러한 포트가 열려 있는지 확인해야 합니다.

SDA 인프라를 활용하는 네트워크에서 어플라이언스를 구축하는 경우에는 추가 포트, 프로토콜 및 트래픽 유형을 수용해야 합니다. 자세한 내용은 필수 SD-Access 포트 및 프로토콜을 참조하십시오.

참고 Cisco DNA Center 구축 시 주의해야 하는 보안 고려 사항에 대한 내용은 Cisco Digital Network Architecture Center 보안 모범 사례 가이드를 참조하십시오.

표 ***8:*** 포트*:* 수신 트래픽

| 포트 번호 | 허용되는 트래픽 | 프로토콜**(TCP** 또는 **UDP)** |
|---|---|---|
| 2222 | SSH | TCP |
| 80 | HTTP | TCP |
| 123 | NTP | UDP |
| 162 | SNMP | UDP |
| 443 | HTTPS | TCP |

표 ***9:*** 포트*:* 발신 트래픽

| 포트 번호 | 허용되는 트래픽 | 프로토콜**(TCP** 또는 **UDP)** |
|---|---|---|
| 22 | SSH(네트워크 디바이스에 연결) | TCP |
| 23 | 텔넷(네트워크 디바이스에 연결) | TCP |
| 53 | DNS | UDP |

| 포트 번호 | 허용되는 트래픽 | 프로토콜(**TCP** 또는 **UDP**) |
|---|---|---|
| 80 | 포트 80은 발신 프록시 컨피그레이션에 사용할 수 있습니다.<br>또한 구성 마법사에서 프록시를 구성하는 동안(이미 해당 네트워크에서 프록시를 사용 중인 경우) 8080과 같은 다른 일반 포트를 사용할 수도 있습니다.<br>Cisco 지원 인증서 및 신뢰 풀에 액세스하기 위해 어플라이언스에서 다음 URL의 Cisco 주소에 보내는 발신 IP 트래픽을 허용하도록 네트워크를 구성할 수 있습니다.<br>https://www.cisco.com/security/pki/ | TCP |
| 123 | NTP | UDP |
| 161 | SNMP 에이전트 | UDP |
| 443 | HTTPS | TCP |
| 5222 | PxGrid용 ISE XMP | TCP |
| 9060 | ISE ERS API 트래픽 | TCP |

다음 표에는 어플라이언스에 대한 수신 IP 트래픽을 허용하는 포트가 나와 있습니다.

표 ***10:*** 포트***: IP*** 트래픽

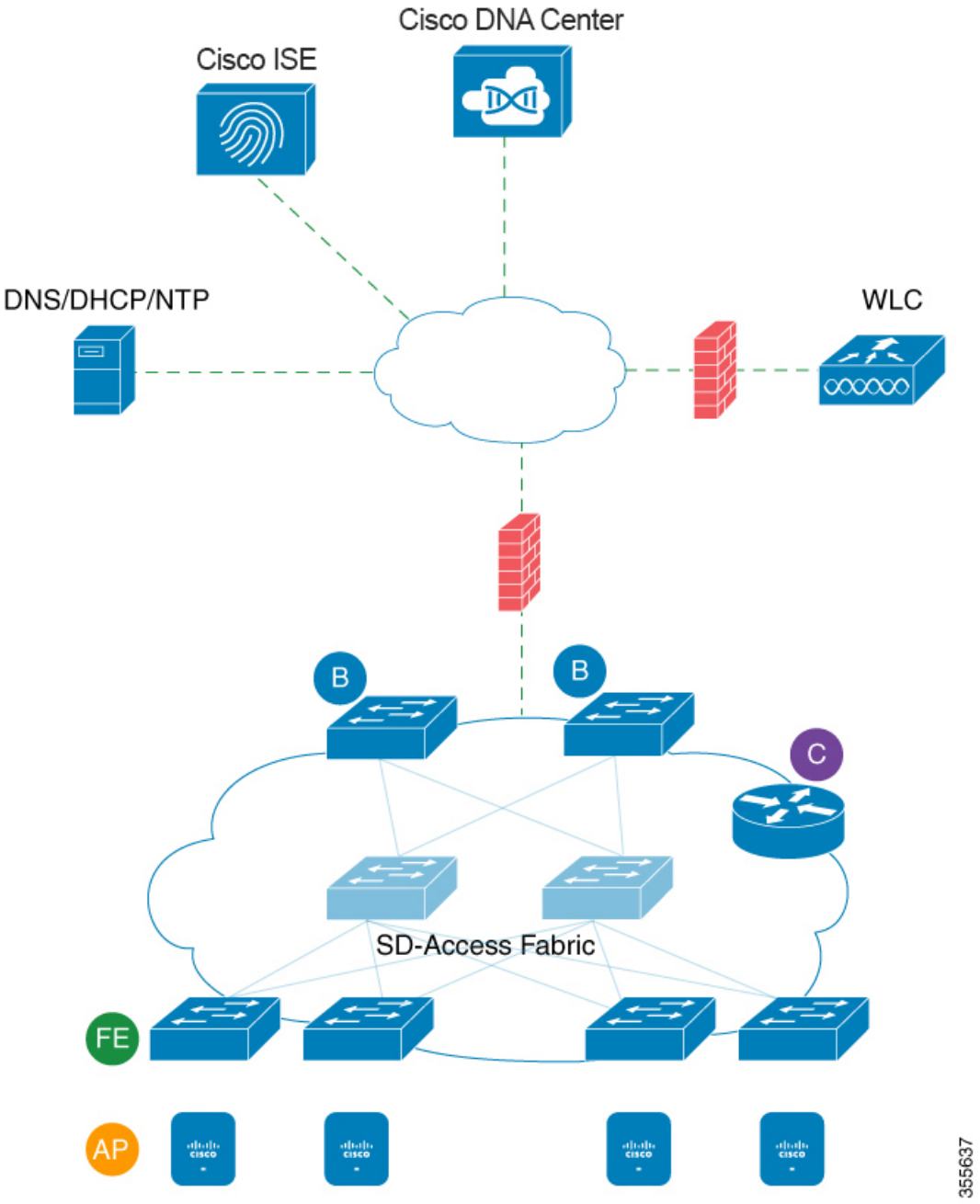
| 프로토콜(**TCP** 또는 **UDP**) | 포트 번호 | 트래픽 유형 |
|---|---|---|
| TCP | 22 | SSH |
| TCP | 2222 | SSH |
| TCP | 80 | HTTP |
| TCP | 443 | HTTPS |
| UDP | 67 | bootps |
| UDP | 123 | NTP |
| UDP | 162 | SNMP |

또한 어플라이언스에서 다음 URL의 Cisco 주소에 보내는 발신 IP 트래픽을 허용하도록 네트워크를 구성할 수도 있습니다. https://www.cisco.com/security/pki/ 어플라이언스에서는 위 URL에 나열된 IP 주소를 Cisco 지원 인증서 및 신뢰 풀에 액세스하는 데 사용합니다.

# 필수 SD-Access 포트 및 프로토콜

이 항목에는 아래 그림에 나와 있는 것과 같은 일반 SDA 패브릭 구축을 기본으로 하는 포트, 프로토콜 및 트래픽 유형에 대해 자세히 설명되어 있습니다.

그림 ***5: SDA*** 패브릭 인프라




네트워크에서 SDA를 구현한 경우, 다음 표의 정보를 사용하여 네트워크 관리를 자동화하는 데 필요한 액세스 권한을 Cisco DNA Center에 제공하면서 SDA 인프라를 적절하게 보호하는 방화벽 및 보안 정책을 계획합니다.

표 ***11: Cisco DNA Center*** 트래픽

| 소스 포트[2] | 소스 | **Destination Port(**목적지 포트**)** | 대상 | 설명 |
|---|---|---|---|---|
| Any(모든) | Cisco DNA Center | UDP 53 | DNS Server(DNS 서버) | Cisco DNA Center에서 DNS 서버로 |
| Any(모든) | Cisco DNA Center | TCP 22 | 패브릭 언더레이 | Cisco DNA Center에서 SSH를 위한 패브릭 스위치의 루프백으로 |
| Any(모든) | Cisco DNA Center | TCP 23 | 패브릭 언더레이 | Cisco DNA Center에서 TELNET를 위한 패브릭 스위치의 루프백으로 |
| Any(모든) | Cisco DNA Center | UDP 161 | 패브릭 언더레이 | Cisco DNA Center에서 SNMP 디바이스 검색을 위한 패브릭 스위치의 루프백으로 |
| ICMP | Cisco DNA Center | ICMP | 패브릭 언더레이 | Cisco DNA Center에서 SNMP 디바이스 검색을 위한 패브릭 스위치의 루프백으로 |
| Any(모든) | Cisco DNA Center | TCP 443 | 패브릭 언더레이 | Cisco DNA Center에서 소프트웨어 업그레이드를 위한 패브릭 스위치로(프록시가 없는 경우 인터넷으로도) |
| Any(모든) | Cisco DNA Center | TCP 80 | 패브릭 언더레이 | Cisco DNA Center에서 PnP를 위한 패브릭 스위치로(프록시가 없는 경우 인터넷으로도) |
| Any(모든) | Cisco DNA Center | TCP 830 | 패브릭 언더레이 | Cisco DNA Center에서 Netconf를 위한 패브릭 스위치로(SDA 임베디드 무선) |
| UDP 123 | Cisco DNA Center | UDP 123 | 패브릭 언더레이 | LAN 자동화 시 초기 시간을 위해 Cisco DNA Center에서 패브릭 스위치로 |
| Any(모든) | Cisco DNA Center | UDP 123 | NTP 서버 | Cisco DNA Center에서 NTP 서버로 |
| Any(모든) | Cisco DNA Center | TCP 22, UDP 161 | WLC | Cisco DNA Center에서 WLC로 |
| ICMP | Cisco DNA Center | ICMP | WLC | Cisco DNA Center에서 WLC로 |
| Any(모든) | Cisco DNA Center | TCP 80, TCP 443 | AP | Cisco DNA Center에서 AP로(센서 및 활성 센서로서)(Cisco Aironet 1800S) |

| | | | | |
|---|---|---|---|---|
| Any(모든) | Cisco DNA Center | TCP 32626 | AP | Cisco DNA Center에서 gRPC용 AP로 |

[2] 클러스터, PKI, SFTP 서버 및 프록시 포트 트래픽은 이 표에 포함되어 있지 않습니다.

표 ***12:*** 인터넷 연결 트래픽

| **Source Port(**소스 포트**)** | 소스 | **Destination Port(**목적지 포트**)** | 대상 | 설명 |
|---|---|---|---|---|
| Any(모든) | Cisco DNA Center | TCP 443 | registry.ciscoconnectdna.com | Cisco DNA Center 패키지 업데이트 다운로드 |
| Any(모든) | Cisco DNA Center | TCP 443 | www.ciscoconnectdna.com | Cisco DNA Center 패키지 업데이트 다운로드 |
| Any(모든) | Cisco DNA Center | TCP 443 | registry-cdn.ciscoconnectdna.com | Cisco DNA Center 패키지 업데이트 다운로드 |
| Any(모든) | Cisco DNA Center | TCP 443 | cdn.ciscoconnectdna.com | Cisco DNA Center 패키지 업데이트 다운로드 |
| Any(모든) | Cisco DNA Center | TCP 443 | software.cisco.com | 디바이스 소프트웨어 다운로드 |
| Any(모든) | Cisco DNA Center | TCP 443 | cloudsso.cisco.com | Cisco.com 및 스마트 어카운트 크리덴셜 검증 |
| Any(모든) | Cisco DNA Center | TCP 443 | cloudsso1.cisco.com | Cisco.com 및 스마트 어카운트 크리덴셜 검증 |
| Any(모든) | Cisco DNA Center | TCP 443 | cloudsso2.cisco.com | Cisco.com 및 스마트 어카운트 크리덴셜 검증 |
| Any(모든) | Cisco DNA Center | TCP 443 | apiconsole.cisco.com | CSSM Smart Licensing API |
| Any(모든) | Cisco DNA Center | TCP 443 | sso.cisco.com | CCO 및 Smart Licensing |
| Any(모든) | Cisco DNA Center | TCP 443 | api.cisco.com | CCO 및 Smart Licensing |
| Any(모든) | Cisco DNA Center | TCP 443 | apx.cisco.com | CCO 및 Smart Licensing |
| Any(모든) | Cisco DNA Center | TCP 443 | dashboard.meraki.com | Meraki 통합 |
| Any(모든) | Cisco DNA Center | TCP 443 | api.meraki.com | Meraki 통합 |
| Any(모든) | Cisco DNA Center | TCP 443 | n63.meraki.com | Meraki 통합 |

| | | | | |
|---|---|---|---|---|
| Any(모든) | Cisco DNA Center | TCP 443 | dnacenter.uservoice.com | 사용자 피드백 제출 |
| Any(모든) | Cisco DNA Center 관리 클라이언트 | TCP 443 | *.tiles.mapbox.com | 브라우저에서 맵 렌더링(프록시를 통해 액세스하는 경우 대상은 *.tiles.mapbox.com/*) |
| Any(모든) | Cisco DNA Center | TCP 443 | www.mapbox.com | 맵 및 WLC 국가 코드 식별 |

표 ***13: SDA*** 패브릭 언더레이 트래픽

| 소스 포트[3] | 소스 | **Destination Port(**목적지 포트**)** | 대상 | 설명 |
|---|---|---|---|---|
| UDP 68 | 패브릭 언더레이 | UDP 67 | DHCP 서버 | 패브릭 에지 노드에 의해 시작되는 DHCP 릴레이 패킷을 위해 패브릭 스위치 및 라우터에서 DHCP 서버로 |
| Any(모든) | 패브릭 언더레이 | TCP 80 | Cisco DNA Center | PnP를 위해 패브릭 스위치 및 라우터 루프백 IP에서 Cisco DNA Center로 |
| Any(모든) | 패브릭 언더레이 | TCP 443 | Cisco DNA Center | 이미지 업그레이드를 위해 패브릭 스위치 및 라우터 루프백 IP에서 Cisco DNA Center로 |
| Any(모든) | 패브릭 언더레이 | UDP 162 | Cisco DNA Center | SNMP 트랩을 위해 패브릭 스위치 및 라우터 루프백 IP에서 Cisco DNA Center로 |
| Any(모든) | 패브릭 언더레이 | UDP 514 | Cisco DNA Center | 어슈어런스를 위해 패브릭 스위치와 라우터에서 Cisco DNA Center로 |
| Any(모든) | 패브릭 언더레이 | UDP 6007 | Cisco DNA Center | NetFlow를 위해 패브릭 라우터에서 Cisco DNA Center로 |
| Any(모든) | 패브릭 언더레이 | UDP 123 | Cisco DNA Center | 패브릭 스위치에서 Cisco DNA Center로, LAN 자동화를 수행할 때 사용됨 |
| ICMP | 패브릭 언더레이 | ICMP | Cisco DNA Center | SNMP를 위해 패브릭 스위치 및 라우터 루프백에서 Cisco DNA Center로: 디바이스 검색 |
| UDP 161 | 패브릭 언더레이 | Any(모든) | Cisco DNA Center | SNMP를 위해 패브릭 스위치 및 라우터 루프백에서 Cisco DNA Center로: 디바이스 검색 |

| | | | | |
|---|---|---|---|---|
| Any(모든) | 패브릭 언더레이 | UDP 53 | DNS Server(DNS 서버) | 이름 확인을 위해 패브릭 스위치 및 라우터에서 DNS 서버로 |
| TCP 및 UDP 4342 | 패브릭 언더레이 | TCP 및 UDP 4342 | 패브릭 라우터 및 스위치 | LISP 캡슐화된 제어 메시지 |
| TCP 및 UDP 4342 | 패브릭 언더레이 | Any(모든) | 패브릭 라우터 및 스위치 | LISP 제어 평면 통신 |
| Any(모든) | 패브릭 언더레이 | UDP 4789 | 패브릭 라우터 및 스위치 | 패브릭 캡슐화된 데이터 패킷(VXLAN-GPO) |
| Any(모든) | 패브릭 언더레이 | UDP 1645/1646/1812/1813 | ISE | RADIUS를 위해 패브릭 스위치 및 라우터 루프백 IP에서 ISE로 |
| ICMP | 패브릭 언더레이 | ICMP | ISE | 트러블슈팅을 위해 패브릭 스위치와 라우터에서 ISE로 |
| UDP 1700/3799 | 패브릭 언더레이 | Any(모든) | ISE | COA를 위해 패브릭 스위치에서 ISE로 |
| Any(모든) | 패브릭 언더레이 | UDP 123 | NTP 서버 | 패브릭 스위치 및 라우터 루프백 IP에서 NTP 서버로 |
| Any(모든) | control-plane | UDP 및 TCP 4342/4343 | WLC | 패브릭 활성화 무선을 위해 제어 평면 루프백 IP에서 WLC로 |

[3] 보더 라우팅 프로토콜, SPAN, 프로파일링 및 텔레메트리 트래픽은 이 표에 포함되어 있지 않습니다.

표 ***14: WLC(Wireless LAN Controller)*** 트래픽

| **Source Port(**소스 포트**)** | 소스 | **Destination Port(**목적지 포트**)** | 대상 | 설명 |
|---|---|---|---|---|
| UDP 5246/5247/5248 | WLC | Any(모든) | AP IP 풀 | CAPWAP를 위해 WLC에서 AP 서브넷으로 |
| ICMP | WLC | ICMP | AP IP 풀 | 트러블슈팅을 위해 WLC에서 Ping을 허용하는 AP로 |
| Any(모든) | WLC | UDP 69/5246/5247 TCP 22 | AP IP 풀 | CAPWAP에 대한 WLC에서 AP 서브넷으로 |
| Any(모든) | WLC | UDP 및 TCP 4342/4343 | 컨트롤 플레인 | WLC에서 제어-평면 루프백 IP로 |
| Any(모든) | WLC | TCP 32222 | Cisco DNA Center | 디바이스 검색을 위해 WLC에서 Cisco DNA Center로 |

| | | | | |
|---|---|---|---|---|
| UDP 161 | WLC | Any(모든) | Cisco DNA Center | SNMP를 위해 WLC에서 Cisco DNA Center로 |
| Any(모든) | WLC | UDP 162 | Cisco DNA Center | SNMP 트랩을 위해 WLC에서 Cisco DNA Center로 |
| Any(모든) | WLC | TCP 16113 | MSE 및 Spectrum Expert | NMSP를 위해 WLC에서 MSE 및 Spectrum Expert로 |
| ICMP | WLC | ICMP | Cisco DNA Center | 트러블슈팅을 위해 WLC에서 Ping을 허용하도록 |
| Any(모든) | HA 서버 | TCP 1315 | Cisco DNA Center | 데이터베이스 서버 HA(QoS) |
| Any(모든) | HA 서버 | TCP 1316–1320 | Cisco DNA Center | HA 데이터베이스 포트 |
| Any(모든) | HA 웹 서버 | TCP 8082 | Cisco DNA Center | HA 웹 서버의 상태 모니터 포트 |
| Any(모든) | WLC 및 다양한 Syslog 서버 | UDP 514 | WLC | Syslog(선택 사항) |
| Any(모든) | WLC | UDP 53 | DNS Server(DNS 서버) | WLC에서 DNS 서버로 |
| Any(모든) | WLC | TCP 443 | ISE | 게스트 SSID 웹 권한 부여를 위해 WLC에서 ISE로 |
| Any(모든) | WLC | UDP 1645,1812 | ISE | RADIUS 인증을 위해 WLC에서 ISE로 |
| Any(모든) | WLC | UDP 1646, 1813 | ISE | RADIUS 어카운팅을 위해 WLC에서 ISE로 |
| Any(모든) | WLC | UDP 1700, 3799 | ISE | RADIUS CoA를 위해 WLC에서 ISE로 |
| ICMP | WLC | ICMP | ISE | 트러블슈팅을 위해 WLC에서 ISE ICMP로 |
| Any(모든) | WLC | UDP 123 | NTP 서버 | WLC에서 NTP 서버로 |

표 ***15:*** 패브릭 활성화 무선 ***AP(***액세스 포인트***) IP*** 풀 트래픽

| **Source Port(**소스 포트**)** | 소스 | **Destination Port(**목적지 포트**)** | 대상 | 설명 |
|---|---|---|---|---|
| UDP 68 | AP IP 풀 | UDP 67 | DHCP 서버 | AP IP 풀에서 DHCP 서버로 |

| | | | | |
|---|---|---|---|---|
| ICMP | AP IP 풀 | ICMP | DHCP 서버 | 트러블슈팅을 위해 AP IP 풀에서 ICMP로 |
| Any(모든) | AP IP 풀 | 514 | 다수 | Syslog - 대상을 구성할 수 있습니다. 기본값은 255.255.255.255입니다. |
| Any(모든) | AP IP 풀 | UDP 69/5246/5247/5248 | WLC | CAPWAP를 위해 AP IP 풀에서 WLC로 |
| ICMP | AP IP 풀 | ICMP | WLC | AP IP 풀에서 트러블슈팅을 위해 Ping을 허용하는 WLC로 |

표 ***16: ISE(Identity Services Engine)*** 트래픽

| 소스 포트[4] | 소스 | **Destination Port(**목적지 포트**)** | 대상 | 설명 |
|---|---|---|---|---|
| Any(모든) | ISE | TCP 64999 | 경계 | SXP를 위해 ISE에서 보더 노드로 |
| Any(모든) | ISE | UDP 514 | Cisco DNA Center | ISE에서 Syslog 서버로(Cisco DNA Center) |
| UDP 1645/1646/1812/1813 | ISE | Any(모든) | 패브릭 언더레이 | RADIUS 및 권한 부여를 위해 ISE에서 패브릭 스위치 및 라우터로 |
| Any(모든) | ISE | UDP 1700/3799 | 패브릭 언더레이 | 주소 관리를 위해 ISE에서 패브릭 스위치 및 라우터 루프백 IP로 |
| ICMP | ISE | ICMP | 패브릭 언더레이 | 트러블슈팅을 위해 ISE에서 패브릭 스위치로 |
| Any(모든) | ISE | UDP 123 | NTP 서버 | ISE에서 NTP 서버로 |
| UDP 1812/1645/1813/1646 | ISE | Any(모든) | WLC | RADIUS를 위해 ISE에서 WLC로 |
| ICMP | ISE | ICMP | WLC | 트러블슈팅을 위해 ISE에서 WLC로 |

[4] 참고: 고가용성 및 프로파일링 트래픽은 이 표에 포함되어 있지 않습니다.

표 ***17: DHCP*** 서버 트래픽

| **Source Port(**소스 포트**)** | 소스 | **Destination Port(**목적지 포트**)** | 대상 | 설명 |
|---|---|---|---|---|
| UDP 67 | DHCP 서버 | UDP 68 | AP IP 풀 | DHCP 서버에서 패브릭 AP로 |
| ICMP | DHCP 서버 | ICMP | AP IP 풀 | 트러블슈팅을 위한 ICMP: 패브릭-DHCP |

| | | | | |
|---|---|---|---|---|
| UDP 67 | DHCP 서버 | UDP 68 | 패브릭 언더레이 | DHCP에서 패브릭 스위치 및 라우터로 |
| ICMP | DHCP 서버 | ICMP | 패브릭 언더레이 | 트러블슈팅을 위한 ICMP: 패브릭-DHCP |
| UDP 67 | DHCP 서버 | UDP 68 | 사용자 IP 풀 | DHCP 서버에서 패브릭 스위치 및 라우터로 |
| ICMP | DHCP 서버 | ICMP | 사용자 IP 풀 | 트러블슈팅을 위한 ICMP: 사용자-DHCP |

표 ***18: NTP*** 서버 트래픽

| **Source Port**(소스 포트) | 소스 | **Destination Port**(목적지 포트) | 대상 | 설명 |
|---|---|---|---|---|
| UDP 123 | NTP 서버 | Any(모든) | ISE | NTP 서버에서 ISE로 |
| UDP 123 | NTP 서버 | Any(모든) | Cisco DNA Center | NTP 서버에서 Cisco DNA Center |
| UDP 123 | NTP 서버 | Any(모든) | 패브릭 언더레이 | NTP 서버에서 패브릭 스위치 및 라우터 루프백으로 |
| UDP 123 | NTP 서버 | Any(모든) | WLC | NTP 서버에서 WLC로 |

표 ***19: DNS*** 서버 트래픽

| **Source Port**(소스 포트) | 소스 | **Destination Port**(목적지 포트) | 대상 | 설명 |
|---|---|---|---|---|
| UDP 53 | DNS Server(DNS 서버) | Any(모든) | 패브릭 언더레이 | DNS 서버에서 패브릭 스위치로 |
| UDP 53 | DNS Server(DNS 서버) | Any(모든) | WLC | DNS 서버에서 WLC로 |

# 필수 구성 정보

어플라이언스 구성 시 필수 서브넷 및 추가 IP 주소 외에도 다음과 같은 정보를 입력하라는 프롬프트가 표시됩니다.

1. **Linux User Name(Linux** 사용자 이름**)**: 이는 **`maglev`**입니다. 이 사용자 이름은 마스터 노드 및 추가 기능 노드를 비롯하여 클러스터의 모든 어플라이언스에서 동일하며 변경할 수 없습니다.
2. **Linux Password(Linux** 비밀번호**)**: Linux 사용자 이름인 **`maglev`**에 대한 비밀번호를 식별합니다. 이 비밀번호는 Linux 명령줄을 통해 각 어플라이언스에 대한 보안 액세스를 보장합니다. 원하는

경우 클러스터의 각 어플라이언스에서 각 **maglev** Linux 사용자 이름에 대해 서로 다른 Linux 비밀번호를 할당할 수 있습니다.

기본값이 없으므로 Linux 비밀번호를 생성해야 합니다. 비밀번호는 다음 요건을 충족해야 합니다.

- 8자 이상입니다.
- 탭 또는 줄 바꿈을 포함하지 않습니다.
- 다음 범주 중 3개 이상의 문자를 포함합니다.
  - 대문자
  - 소문자
  - 숫자
  - 특수 문자(예: !, #)

Linux 비밀번호는 Cisco DNA Center 데이터베이스에서 암호화되고 해싱됩니다. 다중 노드 클러스터를 구축하는 경우에는 각 추가 기능 노드에서 마스터 노드의 Linux 비밀번호를 입력하라는 프롬프트도 표시됩니다.

3. **Password Generation Seed (Optional)**(비밀번호 생성 시드(선택 사항)): Linux 비밀번호를 만들어 내는 대신 시드 구문을 입력하고 **Generate Password**(비밀번호 생성)를 누를 수 있습니다. Maglev 구성 마법사에서는 이 시드 구문을 사용하여 임의의 보안 비밀번호를 생성합니다. **Auto Generated Password**(자동으로 생성된 비밀번호) 필드를 사용하여 생성된 비밀번호를 추가로 수정할 수 있습니다.

4. **Administrator Passphrase**(관리자 암호): 클러스터에서 Cisco DNA Center에 대한 웹 액세스에 사용되는 비밀번호를 식별합니다. 이는 처음으로 Cisco DNA Center에 로그인하는 데 사용하는 수퍼 사용자 어카운트인 **admin**에 대한 비밀번호입니다(최초 로그인 참조). 보안을 유지하기 위해 처음 로그인할 때 이 비밀번호를 변경하라는 프롬프트가 표시됩니다.

   이 비밀번호는 기본값이 없으므로 만들어야 합니다. 관리자 암호는 위에서 설명한 Linux 비밀번호와 동일한 요건을 충족해야 합니다.

5. **CIMC User Password**(CIMC 사용자 비밀번호): CIMC 그래픽 유저 인터페이스에 액세스하는 데 사용되는 비밀번호를 식별합니다. 공장 기본값은 *password*이지만 웹 브라우저를 통해 액세스하기 위해 CIMC를 처음으로 설정할 때 이를 변경하라는 프롬프트가 표시됩니다(CIMC에 대한 브라우저 액세스 활성화 참조).

   CIMC 사용자 비밀번호는 위에서 설명한 Linux 비밀번호와 동일한 요건을 충족해야 합니다. 공장 기본값으로 재설정하는 경우에만 *password*로 다시 변경할 수 있습니다.

6. **Master Node IP Address**(마스터 노드 IP 주소): 클러스터에 추가 기능 노드를 설치하는 경우에만 필요합니다. 이는 마스터 노드에 있는 클러스터 포트의 IP 주소입니다(인터페이스 케이블 연결 참조).

# 필수 초기 설정 정보

어플라이언스의 구성을 완료하고 나면, 처음으로 Cisco DNA Center에 로그인하여 필수 설정 작업을 완료합니다. 이렇게 처음 설정할 때는 다음과 같은 정보가 필요합니다.

1. **New Admin Superuser Password(**새 관리 수퍼 사용자 비밀번호**)**: Cisco DNA Center 관리 수퍼 사용자의 새 비밀번호를 입력하라는 프롬프트가 표시됩니다. 수퍼 사용자 비밀번호를 재설정하면 운영 보안이 향상됩니다. 이는 Cisco DNA Center 어플라이언스를 설치 및 구성한 엔터프라이즈 직원이 Cisco DNA Center 사용자 또는 관리자가 아닌 경우에 특히 중요합니다.
2. **Cisco.com Credentials(Cisco.com** 크리덴셜**)**: 해당 조직에서 소프트웨어 다운로드를 등록하고 이메일을 통해 시스템 통신을 수신하는 데 사용하는 Cisco.com 사용자 ID 및 비밀번호입니다.
3. **Cisco Smart Account Credentials(Cisco** 스마트 어카운트 크리덴셜**)**: 해당 조직에서 디바이스 및 소프트웨어 라이선스를 관리하는 데 사용하는 Cisco.com 스마트 어카운트 사용자 ID 및 비밀번호입니다.
4. **IP Address Manager URL and Credentials(IP** 주소 관리자 **URL** 및 크리덴셜**)**: Cisco DNA Center에서 사용하려는 타사 IPAM(IP 주소 관리자) 서버의 호스트 이름, URL, 관리자 사용자 이름 및 관리자 비밀번호입니다. 현재 릴리스에서는 InfoBlox 또는 Bluecat을 지원합니다.
5. **Proxy URL, Port and Credentials(**프록시 **URL,** 포트 및 크리덴셜**)**: Cisco DNA Center에서 Cisco DNA Center 소프트웨어에 대한 업데이트를 가져오고 디바이스 라이선스를 관리하고 기타 다운로드 가능한 콘텐츠를 검색하기 위해 사용하려는 프록시 서버의 URL(호스트 이름 또는 IP 주소), 포트 번호, 사용자 이름 및 사용자 비밀번호입니다.
6. **Cisco DNA Center Users(**사용자**)**: 생성할 새 Cisco DNA Center 사용자에 대한 사용자 이름, 비밀번호 및 권한 설정입니다. 모든 일반 Cisco DNA Center 운영에 대해 항상 이러한 새 사용자 어카운트 중 하나를 사용하는 것이 좋습니다. 관리 수퍼 사용자 어카운트를 사용하여 Cisco DNA Center 재구성 및 수퍼 사용자 권한이 명시적으로 필요한 기타 작업을 수행하지 마십시오.

이 정보를 입력하라는 프롬프트를 표시하는 최초 설정 마법사를 실행하고 응답하는 방법에 대한 자세한 내용은 최초 로그인을 참조하십시오.

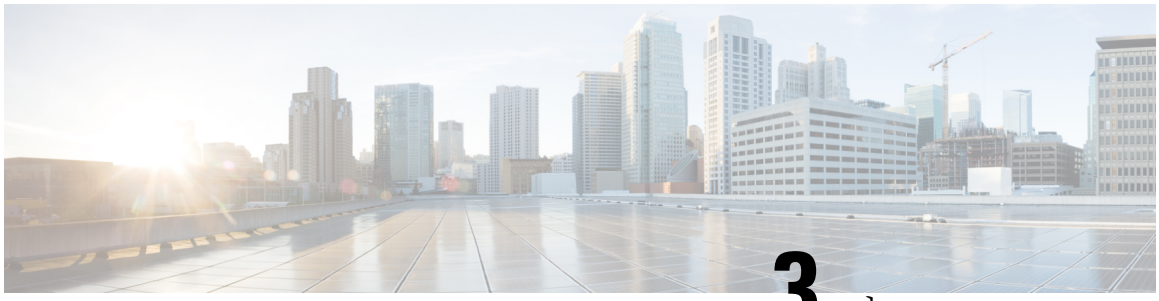
또한 나머지 설정 작업을 완료하려면 다음과 같은 정보가 필요하며, 이러한 작업은 첫 번째 로그인 후에 수행할 수 있습니다.

1. **ISE Server IP and Credentials(ISE** 서버 **IP** 및 크리덴셜**)**: Cisco ISE(Identify Services Engine) 서버 IP 주소, 관리 사용자 이름 및 비밀번호가 필요합니다. 이러한 항목은 Cisco ISE 통합 Cisco DNA Center에 설명된 대로, 해당 조직의 ISE 서버에 로그인한 후 해당 서버에서 Cisco DNA Center와 데이터를 공유하도록 구성하는 데 필요합니다.
2. **Authorization and Policy Server Information(**권한 부여 및 정책 서버 정보**):** Cisco ISE를 인증 및 정책 서버로 사용하는 경우, 위의 ISE 통합에 대한 동일한 정보와 함께 ISE CLI 사용자 이름, CLI 비밀번호, 서버 FQDN, 가입자 이름(예: `cdnac`), ISE SSH 키(선택 사항), 프로토콜 선택 사항(RADIUS 또는 TACACS), 인증 포트, 어카운팅 포트 및 재시도/시간 제한 설정이 필요합니다.

   다른 권한 부여 및 정책 서버를 사용하는 경우에는 서버의 IP 주소, 프로토콜 선택 사항(RADIUS 또는 TACACS), 인증 포트, 어카운팅 포트 및 재시도/시간 제한 설정이 필요합니다.

인증 및 정책 서버 구성에 설명된 대로 이 정보를 사용하여 Cisco DNA Center를 선택한 인증 및 정책 서버와 통합합니다.

3. **SNMP Retry and Timeout Values(SNMP** 재시도 및 시간 제한 값**)**: SNMP 속성 구성에 설명된 대로 디바이스 폴링 및 모니터링을 설정하는 데 필요합니다.



3 장

# 어플라이언스 설치


- 어플라이언스 설치 워크플로, 39 페이지
- 어플라이언스 포장 풀기 및 검사, 40 페이지
- 설치 경고 및 지침 검토, 41 페이지
- 랙 요건 검토, 42 페이지
- 어플라이언스 연결 및 전원 켜기, 42 페이지
- LED 확인, 43 페이지


## 어플라이언스 설치 워크플로

다음 표에는 물리적 설치 작업 및 이 작업을 수행하는 순서에 대해 설명되어 있습니다. 설치하는 각 Cisco DNA Center 어플라이언스에 대해 다음 단계를 수행합니다. 첫 번째 마스터 노드를 구성하기 전에 모든 어플라이언스를 설치해야 합니다.

이 표의 모든 작업을 완료했으면 어플라이언스 구성 워크플로의 단계에 따라 계속 진행합니다.

Cisco DNA Center 어플라이언스 꺼내기, 설치 및 구성 프로세스를 설명하는 비디오를 보려면 이 링크를 클릭하십시오.

표 ***20: Cisco DNA Center*** 어플라이언스 설치 작업

| 단계 | 설명 |
|---|---|
| 1 | 구성 및 설정 시 제공해야 하는 정보를 수집하는 등 다음과 같은 구축 계획 요건을 검토하고 다룹니다.<br>• Cisco DNA Center 및 소프트웨어 정의 액세스 정보<br>• 인터페이스 케이블 연결<br>• 필수 서브넷 및 추가 IP 주소<br>• 필수 인터넷 URL 및 FQDN(Fully Qualified Domain Name)<br>• 인터넷에 대한 보안 액세스 제공<br>• 필수 네트워크 포트<br>• 필수 구성 정보<br>• 필수 초기 설정 정보 |
| 2 | 다음과 같은 어플라이언스의 기능 및 사양을 검토합니다.<br>• 기능 요약<br>• 전면 패널 및 후면 패널<br>• 제품 외장 사양<br>• 환경 사양<br>• 전원 사양 |
| 3 | 어플라이언스 패키지 풀기: 어플라이언스 포장 풀기 및 검사 |
| 4 | 어플라이언스에 대한 운영 경고 및 지침 검토: 설치 경고 및 지침 검토 |
| 5 | 랙에 어플라이언스 설치: 랙 요건 검토 |
| 6 | 어플라이언스에 전원 연결 및 전원 켜기: 어플라이언스 연결 및 전원 켜기 |
| 7 | 전면 및 후면 패널 LED를 확인하여 어플라이언스의 작동 여부 확인: LED 확인 |

# 어플라이언스 포장 풀기 및 검사

⚠

주의 내부 어플라이언스 구성 요소를 다룰 때 ESD 스트랩을 착용하고 캐리어 에지로만 모듈을 다루어야 합니다.

팁 나중에 어플라이언스를 배송해야 할 경우에 대비하여 배송용 상자를 보관하십시오.

참고 새시는 배송에 앞서 철저한 검사를 받습니다. 배송 중에 손상되거나 어떤 품목이 사라진 경우 즉시 고객 서비스 담당자에게 문의하십시오.

단계 **1** 판지 상자에서 어플라이언스를 꺼내고 모든 포장재를 보관합니다.

단계 **2** 고객 서비스 담당자가 제공한 장비 목록과 배송 품목을 비교합니다. 모든 품목이 도착했는지 확인합니다.

단계 **3** 손상된 부분이 있는지 확인하고 불일치하거나 손상된 곳이 있으면 고객 서비스 담당자에게 알립니다. 다음 정보를 미리 준비하십시오.

- 배송업체 송장 번호(배송 전표 참고)
- 손상된 장치의 모델 및 일련 번호
- 손상에 대한 설명
- 손상이 설치에 미친 영향

# 설치 경고 및 지침 검토

경고! 시스템의 과열을 방지하기 위해 최대 권장 주변 온도인 **35°C(95°F)**를 초과하는 곳에서는 작동하지 마십시오**.** 명령문 1047

경고! 플러그**-**소켓 조합은 기본 분리 디바이스로 사용되므로 항상 접근이 용이해야 합니다**.** 명령문 1019

경고! 이 제품은 건물의 단락**(**과전류**)** 방지 설비를 사용합니다**.** 보호 디바이스는 정격 **250V, 15A** 미만이어야 합니다**.** 명령문 1005

경고! 장비를 설치할 때는 지역/국가 전기 코드 규격을 따라야 합니다**.** 명령문 1074

주의 적절한 공기 흐름을 유지하기 위해 레일 키트를 사용하여 어플라이언스를 랙에 설치합니다. 레일 키트를 사용하지 않고 어플라이언스를 다른 어플라이언스 위에 두거나 "쌓아두면" 어플라이언스 상단의 공기 배출구가 차단되어 과열되고 팬 속도가 빨라져 전력 소비량이 증가하게 됩니다. 레일을 사용하면 어플라이언스 간에 필요한 최소 간격을 유지할 수 있으므로 어플라이언스를 랙에 설치할 때에는 레일 키트 위에 어플라이언스를 마운트하는 것이 좋습니다. 레일 키트를 사용하여 어플라이언스를 마운트할 경우 어플라이언스 간 추가 간격을 유지하지 않아도 됩니다.

주의 철공진 기술을 사용하는 UPS(무중단 전력 공급 장치) 유형은 사용하지 마십시오. 이러한 UPS 유형은 Cisco UCS와 같은 시스템에서 불안정해질 수 있습니다. 그러면 데이터 트래픽 패턴의 변화에 따라 전류 요구량의 변동이 커질 수 있습니다.

어플라이언스를 설치할 때 다음과 같은 지침을 따르십시오.

- 어플라이언스 설치에 앞서 사이트 구성을 계획하고 사이트를 준비합니다. 권장 사이트 계획 및 준비 작업은 *Cisco UCS* 사이트 준비 가이드를 참조하십시오.
- 어플라이언스 서비스 작업과 적절한 공기 흐름을 위해 어플라이언스 주변에 알맞은 공간을 확보합니다. 이 어플라이언스에서는 공기가 전면에서 후면으로 이동합니다.
- 사이트 공조 기능이 환경 사양에 나열된 열 요건을 충족하는지 확인합니다.
- 캐비닛 또는 랙이 랙 요건 검토에 나열된 요건을 충족하는지 확인합니다.
- 사이트 전원이 전원 사양에 나열된 요건을 충족하는지 확인합니다. 가능하다면 UPS를 사용하여 정전으로부터 보호할 수 있습니다.

# 랙 요건 검토

적절한 작동을 위해 어플라이언스를 설치하는 랙이 다음과 같은 요건을 충족해야 합니다.

- 표준 48.3cm(19인치) 너비 4포스트 EIA 랙 - ANSI/EIA-310-D-1992 section 1 English universal hole spacing 규격의 마운팅 포스트 포함
- 랙 포스트 구멍은 0.38인치(9.6mm) 정사각형, 0.28인치(7.1mm) 원형, #12-24 UNC 또는 #10-32 UNC도 가능합니다(제공된 슬라이드 레일 사용 시).
- 서버당 1RU(1.75인치, 44.45mm) 이상의 수직 랙 공간이 확보되어야 합니다.

# 어플라이언스 연결 및 전원 켜기

이 섹션에서는 어플라이언스의 전원을 켜고 작동하는지 확인하는 방법에 대해 설명합니다.

단계 **1** 제공된 전원 코드를 어플라이언스의 각 전력 공급 장치에 연결한 다음, 접지된 AC 전원 콘센트에 전원 코드를 연결합니다. 자세한 내용은 전원 사양을 참조하십시오.

첫 부팅 시 어플라이언스가 대기 전원 상태로 부팅될 때까지 약 2분간 기다립니다.

전원 상태 LED로 전원 상태를 확인할 수 있습니다.

- 꺼짐 - 어플라이언스에 AC 전원이 연결되지 않았습니다.
- 황색 - 어플라이언스가 예비 전원 모드입니다. 전원이 CIMC 및 일부 마더보드 기능에만 공급됩니다.
- 녹색 - 어플라이언스가 주 전원 모드입니다. 모든 어플라이언스 구성 요소에 전원이 공급되고 있습니다.

이러한 어플라이언스 및 기타 어플라이언스 LED에 대한 자세한 내용은 전면 패널 및 후면 패널을 참조하십시오.

단계 **2** 전면 패널의 KVM 커넥터에 연결된 제공된 KVM 케이블을 사용하여 USB 키보드와 VGA 모니터를 서버에 연결합니다. 또는 후면 패널의 VGA 및 USB 포트를 사용할 수 있습니다. 한 번에 하나의 VGA 인터페이스에만 연결할 수 있습니다.

다음에 수행할 작업

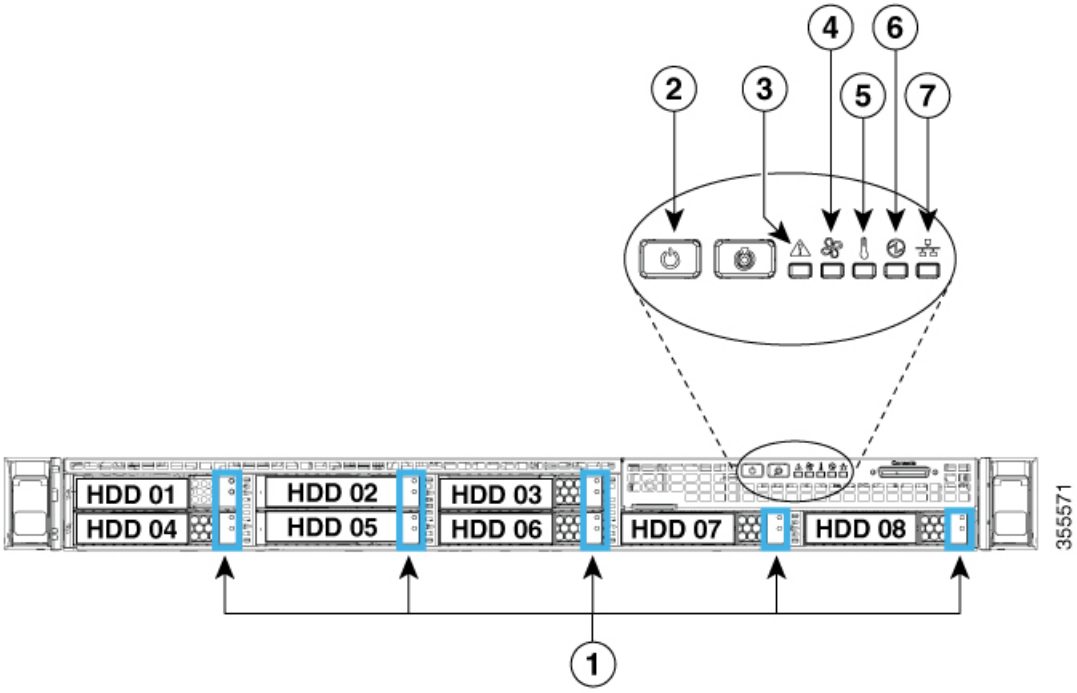
LED 확인에 설명된 절차를 따라 계속 진행합니다.

# LED 확인

Cisco DNA Center 어플라이언스의 전원을 켠 후 전면 패널 및 후면 패널 LED와 버튼의 상태를 확인하여 작동하는지 확인합니다.

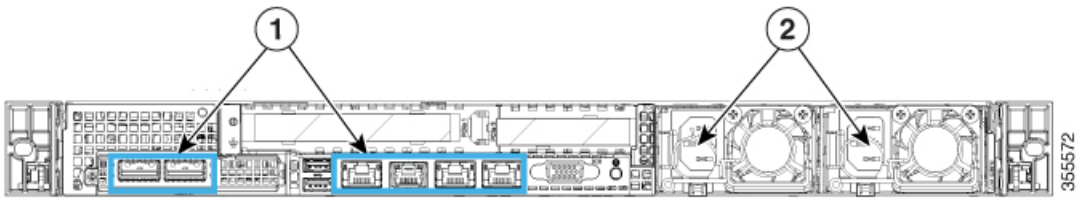
다음 그림에는 물리적 설치 및 첫 번째 전원 켜기를 진행한 후 구성하기 전, Cisco UCS C220 M4 섀시를 사용하는 기능적 어플라이언스의 LED가 나와 있습니다.

그림 *6:* 전면 패널 ***LED***



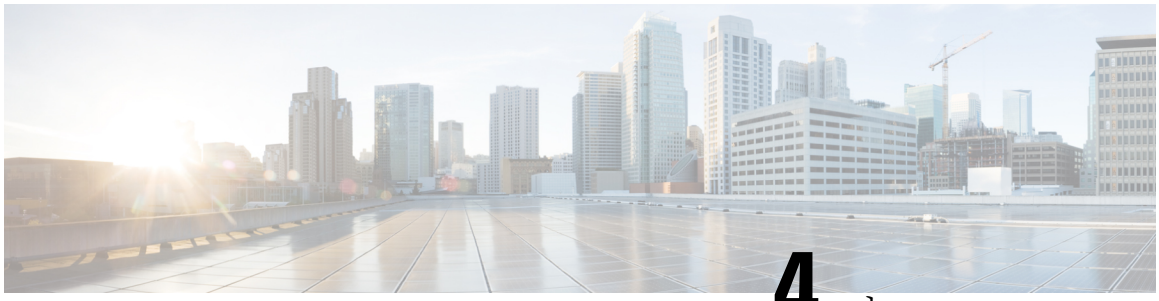

| **LED** | 올바른 상태 표시기 |
|---|---|
| 1 | 드라이브 결함 LED: 꺼짐<br>드라이브 활동 LED: 녹색 |
| 2 | 전원 상태: 녹색 |
| 3 | 시스템 상태: 녹색 |
| 4 | 팬 상태: 녹색 |
| 5 | 온도 상태: 녹색 |
| 6 | 전력 공급 장치 상태: 녹색 |
| 7 | 네트워크 링크 활동: 꺼짐 |

그림 *7:* 후면 패널 ***LED***



| LED | 권장되는 상태 표시기 |
|---|---|
| 1 | 처음 전원을 켤 때 모든 포트의 링크 상태 및 링크 속도 LED가 꺼짐으로 표시되어야 하며 전원 상태 LED는 녹색이어야 합니다.<br><br>Maglev 구성 마법사를 사용하여 네트워크 설정을 구성하고 테스트한 후(마스터 노드 구성 및 추가 기능 노드 구성 참조), 케이블로 연결된 모든 포트에 대한 링크 상태, 링크 속도 및 전원 상태 LED는 녹색이어야 합니다. 케이블이 연결되지 않은 모든 포트 LED는 변경되지 않아야 합니다. |
| 2 | 전력 공급 장치 결함 LED: 꺼짐<br><br>AC 전원 LED: 녹색 |

위에 나와 있는 것 이외의 색상이 나타나는 LED가 표시되면 문제가 있는 상태인 것일 수 있습니다. 이러한 상태를 유발할 수 있는 원인에 대한 자세한 내용은 전면 패널 및 후면 패널을 참조하십시오. 어플라이언스 구성을 진행하기 전에 문제 상태를 해결해야 합니다.



4 장

# 어플라이언스 구성


- 어플라이언스 구성 워크플로, 47 페이지
- CIMC에 대한 브라우저 액세스 활성화, 48 페이지
- 사전 검사 실행, 53 페이지
- Cisco DNA Center ISO 이미지 확인, 60 페이지
- 부팅 가능 USB 드라이브 생성, 61 페이지
- 어플라이언스 이미지 재설치, 62 페이지
- Cisco DNA Center ISO 이미지 설치, 64 페이지
- 마스터 노드 구성, 64 페이지
- 추가 기능 노드 구성, 78 페이지
- 고가용성 클러스터 구축 시나리오, 93 페이지


## 어플라이언스 구성 워크플로

다음 두 가지 모드 중 하나로 네트워크에서 어플라이언스를 구축할 수 있습니다.

- 독립형: 모든 기능을 제공하는 단일 노드입니다. 이 옵션은 일반적으로 초기 또는 테스트 구축 및 소규모 네트워크 환경에 우선 적용됩니다.
- 클러스터: 최대 3개의 노드로 이루어진 클러스터 중 하나입니다. 이 모드에서는 모든 서비스 및 데이터가 호스트 간에 공유됩니다. 이는 대규모 구축에서 우선 적용되는 옵션입니다.

초기 구축을 위해 독립형 모드를 선택하는 경우 나중에 더 많은 어플라이언스를 추가하여 클러스터를 구성할 수 있습니다. 독립형 호스트를 구성할 때는 이를 클러스터에서 첫 번째 또는 마스터 노드로 설정해야 합니다.

초기 구축에 클러스터 모드를 선택하는 경우에는 계속 진행하기 전에 마스터 노드 구성을 완료해야 추가 기능 노드를 구성할 수 있습니다.

다음 표에는 구성 작업 및 이 작업을 수행하는 순서가 자세히 나와 있습니다. 이 표의 작업을 완료했으면 초기 설정 워크플로의 설명에 따라 최초 설정을 완료하여 계속 진행합니다.

어플라이언스 구성 프로세스를 설명하는 비디오를 보려면 이 링크를 클릭하십시오.

표 *21:* 어플라이언스 구성 작업

| 단계 | 설명 |
|---|---|
| 1 | 어플라이언스의 Cisco CIMC(Integrated Management Controller) 그래픽 유저 인터페이스에 대한 브라우저 액세스 활성화: CIMC에 대한 브라우저 액세스 활성화 |
| 2 | 하드웨어 및 스위치 설정 확인 및 조정을 통해 구성에 문제가 없는지 확인: 사전 검사 실행 |
| 3 | CIMC에서 Maglev 구성 마법사 실행 및 클러스터에서 마스터 노드 구성: 마스터 노드 구성 |
| 4 | 3개의 어플라이언스를 설치했으며, 두 번째 및 세 번째 노드를 클러스터에 추가하려는 경우: 추가 기능 노드 구성 |

# CIMC에 대한 브라우저 액세스 활성화

어플라이언스 설치 워크플로에 설명된 대로 어플라이언스를 설치한 후 Cisco IMC Configuration Utility를 사용하여 어플라이언스의 CIMC(Cisco Integrated Management Controller) 포트에 IP 주소 및 게이트웨이를 할당합니다. 이렇게 하면 CIMC 그래픽 유저 인터페이스에 대한 브라우저 액세스가 제공되며, 이 인터페이스는 사용할 어플라이언스를 구성하는 데 사용됩니다.

이 CIMC 설정을 완료한 후에는 CIMC에 로그인하고 올바른 구성을 보장하는 데 도움이 되는 몇 가지 작업을 실행하는 것이 좋습니다(사전 검사 실행 참조).

팁 구축의 보안을 보장하기 위해 CIMC에서는 어플라이언스를 처음 부팅할 때 CIMC 사용자의 기본 비밀번호를 변경하라는 프롬프트를 표시합니다. CIMC 사용자 비밀번호를 나중에 변경하려는 경우 다음과 같이 CIMC GUI를 사용하는 것이 가장 쉽습니다.

1. ☰ > **Admin**(관리자) > **User Management**(사용자 관리) > **Local User**(로컬 사용자)**Management**(관리)를 선택합니다.
2. ID **1**을 선택한 다음, **Modify User**(사용자 수정)를 클릭합니다.

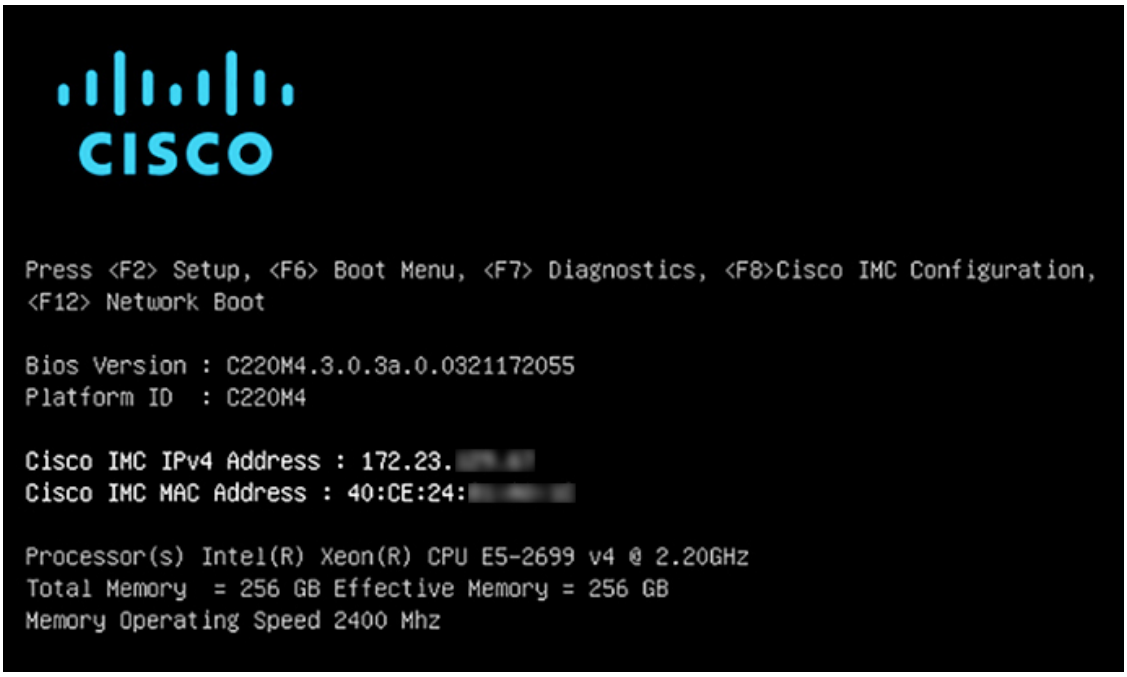
   **Change Password**(비밀번호 변경) 필드에 새 비밀번호를 입력한 다음, **Save**(저장)를 클릭합니다.

단계 **1** 다음 중 하나를 연결하여 어플라이언스 콘솔에 액세스합니다.

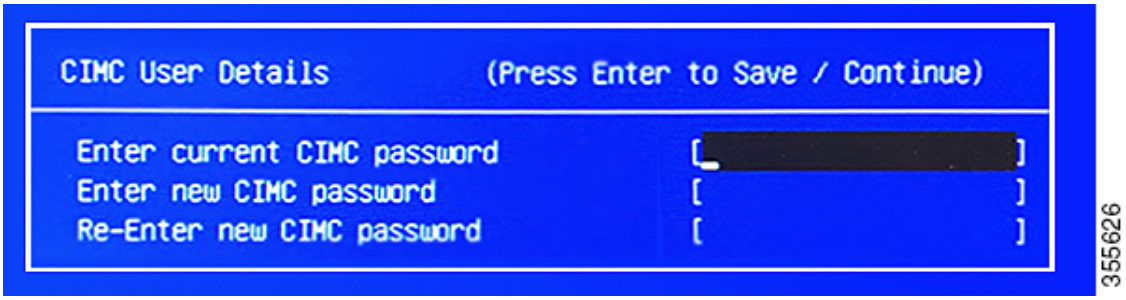
- 어플라이언스 전면 패널의 KVM 커넥터에 대한 KVM 케이블(전면 패널 및 후면 패널에 있는 전면 패널 그림의 구성 요소 12) 또는
- 어플라이언스 후면 패널의 USB 및 VGA 포트(각각 전면 패널 및 후면 패널에 있는 후면 패널 그림의 구성 요소 7 및 12)에 대한 키보드 및 모니터

단계 **2** 어플라이언스의 전원 코드가 연결되어 있고 전원이 켜져 있는지 확인합니다.

단계 **3** 전면 패널의 **Power(**전원**)** 버튼을 눌러 어플라이언스를 부팅합니다. 아래에 표시된 대로 Cisco IMC Configuration Utility 부팅 화면이 표시되는지 확인합니다.

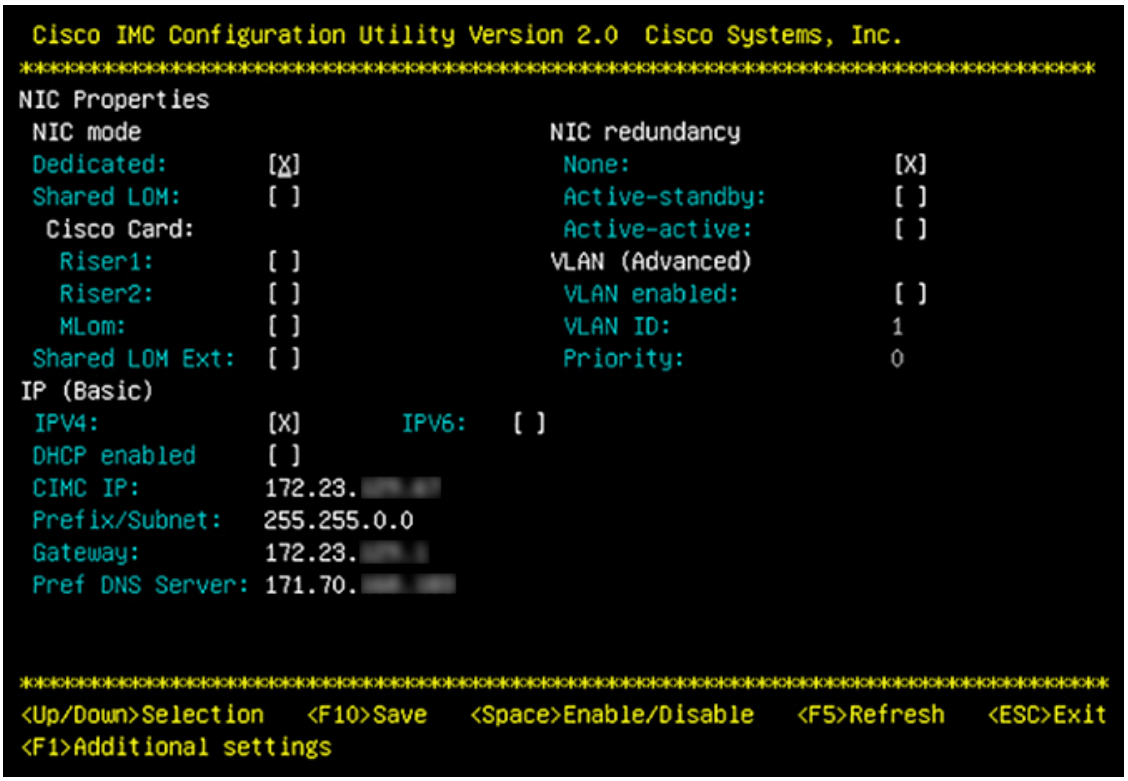



단계 **4** 부팅 화면이 표시되는 즉시 **F8** 키를 눌러 **Cisco IMC Configuration(Cisco IMC** 구성**)**을 수행합니다. Cisco IMC Configuration Utility에 아래에 나와 있는 것과 같은 CIMC 사용자 세부 정보 화면이 표시됩니다.




단계 **5** **Enter current CIMC Password(**현재 **CIMC** 비밀번호 입력**)** 필드에 기본 CIMC 사용자 비밀번호(새 어플라이언스의 기본값은 **password**임)를 입력합니다. 그런 다음 **Enter new CIMC password(**새 **CIMC** 비밀번호 입력**)** 및 **Re-Enter new CIMC password(**새 **CIMC** 비밀번호 재입력**)**에 새 CIMC 사용자 비밀번호를 입력하고 확인합니다.

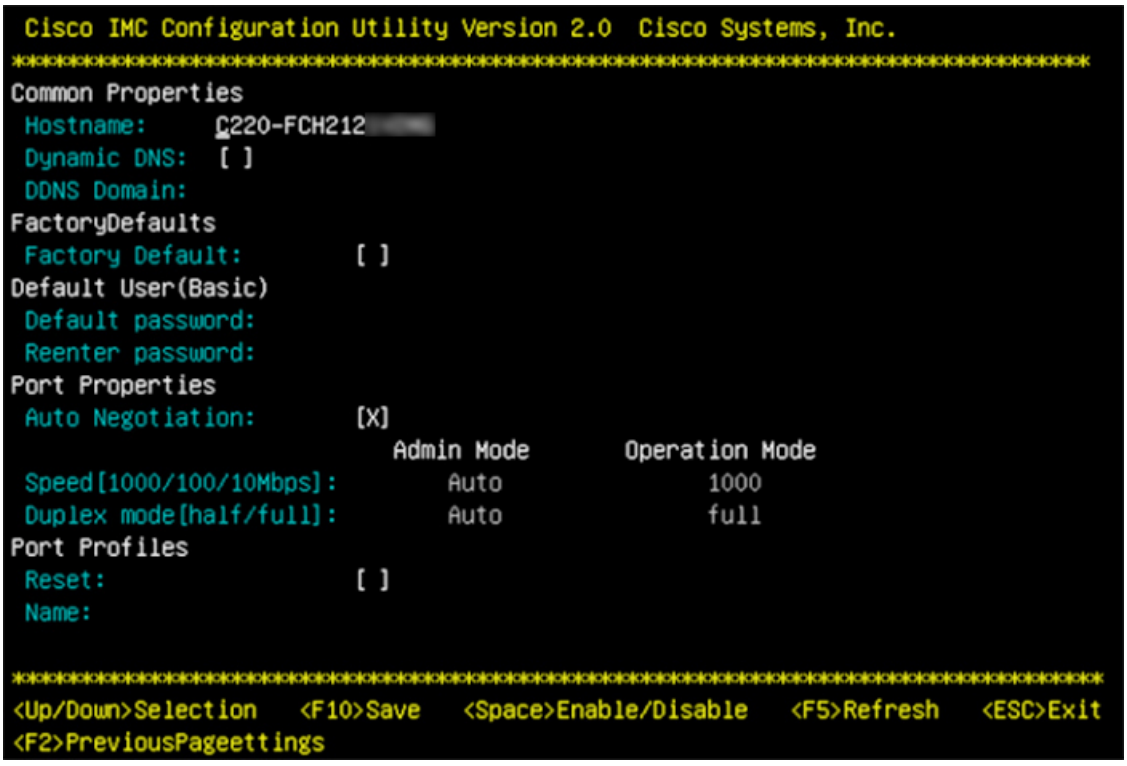
단계 **6** **Re-Enter new CIMC password(**새 **CIMC** 비밀번호 재입력**)**에서 **Enter** 키를 누르면 Cisco IMC Configuration Utility에 아래에 나와 있는 것과 같은 **NIC Properties(NIC** 속성**)** 화면이 표시됩니다.




단계 **7** 다음 변경 작업을 수행합니다.

- **NIC mode(NIC** 모드**) - Dedicated(**전용**)**를 선택합니다.
- **IP(Basic)(IP -** 기본**) - IPV4**를 선택합니다.
- **CIMC IP** - CIMC 포트의 IP 주소를 입력합니다.
- **Prefix/Subnet(**접두사/서브넷**)** - CIMC 포트 IP 주소에 대한 서브넷 마스크를 입력합니다.
- **Gateway(**게이트웨이**)** - 기본 설정된 기본 게이트웨이의 IP 주소를 입력합니다.
- **Pref DNS Server(**기본 **DNS** 서버**)** - 기본 설정된 DNS 서버의 IP 주소를 입력합니다.
- **NIC Redundancy(NIC** 이중화**) - None(**없음**)**을 선택합니다.

단계 **8** **F1** 키를 눌러 **Additional settings(**추가 설정**)**를 지정합니다. Cisco IMC Configuration Utility에 아래에 나와 있는 것과 같은 **Common Properties(**공통 속성**)** 화면이 표시됩니다.




단계 **9** 다음 변경 작업을 수행하십시오.

- **Hostname(**호스트 이름**)**: 이 어플라이언스에서 CIMC에 대한 호스트 이름을 입력합니다.
- **Dynamic DNS(**동적 **DNS)**: 이 기능을 비활성화하려면 체크 박스의 선택을 취소합니다.
- **Factory Defaults(**공장 기본값**)**: 이 기능을 비활성화하려면 체크 박스의 선택을 취소합니다.
- **Default User (Basic)(**기본 사용자**(**기본**))**: 이 필드는 비워둡니다.
- **Port Properties(**포트 속성**)**: 새 설정을 입력하거나 이 필드에 표시된 기본값을 그대로 사용합니다.
- **Port profile(**포트 프로필**)**: 이 기능을 비활성화하려면 체크 박스의 선택을 취소합니다.

단계 **10** **F10** 키를 눌러 설정을 **Save(**저장**)**합니다.

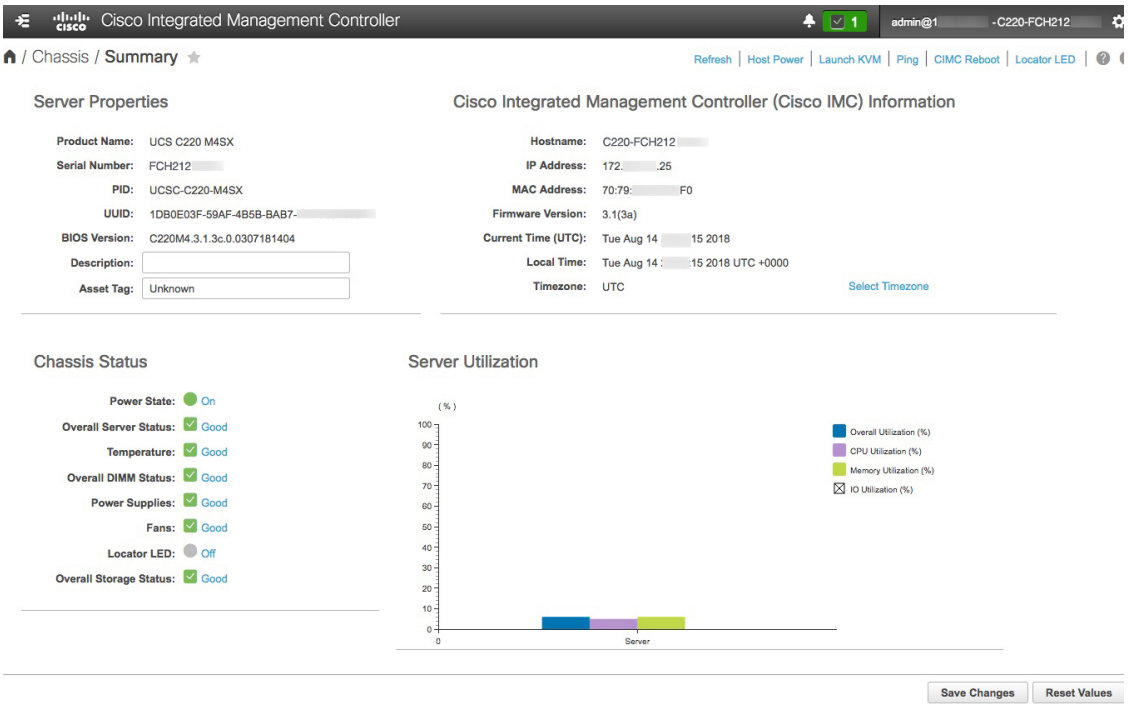
단계 **11** **Escape** 키를 눌러 **Exit(**종료**)**하고 어플라이언스를 리부팅합니다.

단계 **12** 설정이 저장되고 어플라이언스의 리부팅이 완료되면, 어플라이언스가 설치된 서브넷에 대한 액세스 권한이 있는 클라이언트 머신에서 호환되는 브라우저를 열고 다음과 같은 URL을 입력합니다.

**`https://`*`CIMC_ip_address`*(**여기서 ***`CIMC_ip_address`***는 5단계에서 입력한 CIMC 포트 IP 주소)

브라우저에 아래에 나와 있는 것과 같은 기본 Cisco Integrated Management Controller GUI 로그인 창이 표시됩니다.

단계 **13** 5단계에서 설정한 CIMC 사용자 ID 및 비밀번호를 사용하여 로그인합니다. 로그인에 성공하면 브라우저에 아래에 나와 있는 것과 같은 **Cisco Integrated Management Controller** 섀시 요약 창이 표시됩니다.



다음에 수행할 작업

문제 없는 구성을 보장하는 데 도움이 되는 작업 수행: 사전 검사 실행

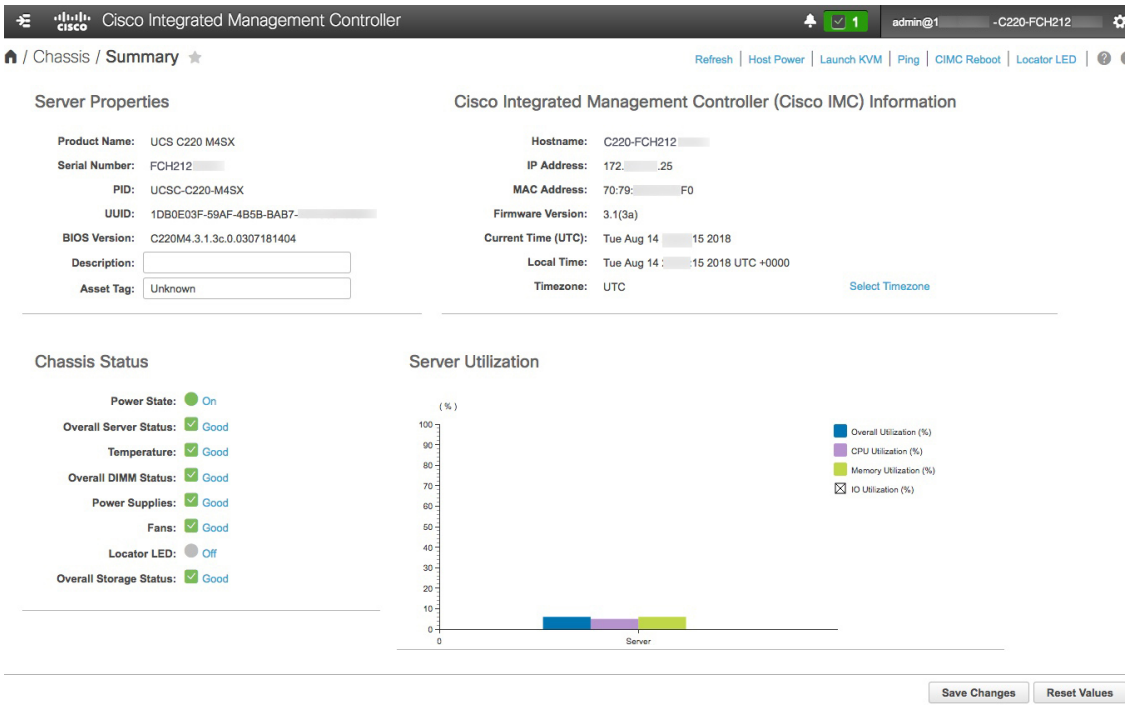
# 사전 검사 실행

어플라이언스 설치 워크플로에 설명된 대로 어플라이언스를 설치하고 CIMC에 대한 브라우저 액세스 활성화에 설명된 대로 CIMC GUI에 대한 액세스를 설정한 후에 CIMC를 사용하여 다음과 같은 사전 구성 작업을 수행합니다. 이러한 작업은 올바른 구성 및 구축을 보장하는 데 도움이 됩니다.

1. 네트워크를 관리하는 데 사용하는 NTP(Network Time Protocol) 서버와 어플라이언스 하드웨어를 동기화합니다. 이는 필수 서브넷 및 추가 IP 주소에 설명된 대로 구현을 계획할 때 사용하기 위해 수집한 호스트 이름 또는 IP가 있는 동일한 NTP 서버여야 합니다. 이 작업은 Cisco DNA Center 데이터가 네트워크 전체에서 올바르게 동기화되도록 보장하는 중요한 작업입니다.
2. 어플라이언스의 10Gbps 포트가 활성화되어 있으며 높은 처리량에 맞게 적절하게 구성되어 있는지 확인합니다.
3. 더 높은 처리량 설정을 지원하도록 10Gbps 어플라이언스 포트에 연결된 스위치를 재구성합니다.
4. 크기가 큰 802.1p 프레임을 지원하도록 10Gbps 어플라이언스 포트에 연결된 스위치를 재구성합니다.

---

단계 **1** CIMC에 대한 브라우저 액세스 활성화에서 설정한 CIMC IP 주소, 사용자 ID 및 비밀번호를 사용하여 어플라이언스의 CIMC에 로그인합니다. 로그인에 성공하면 브라우저에 아래에 나와 있는 것과 같은 **Cisco Integrated Management Controller** 새시 요약 창이 표시됩니다.

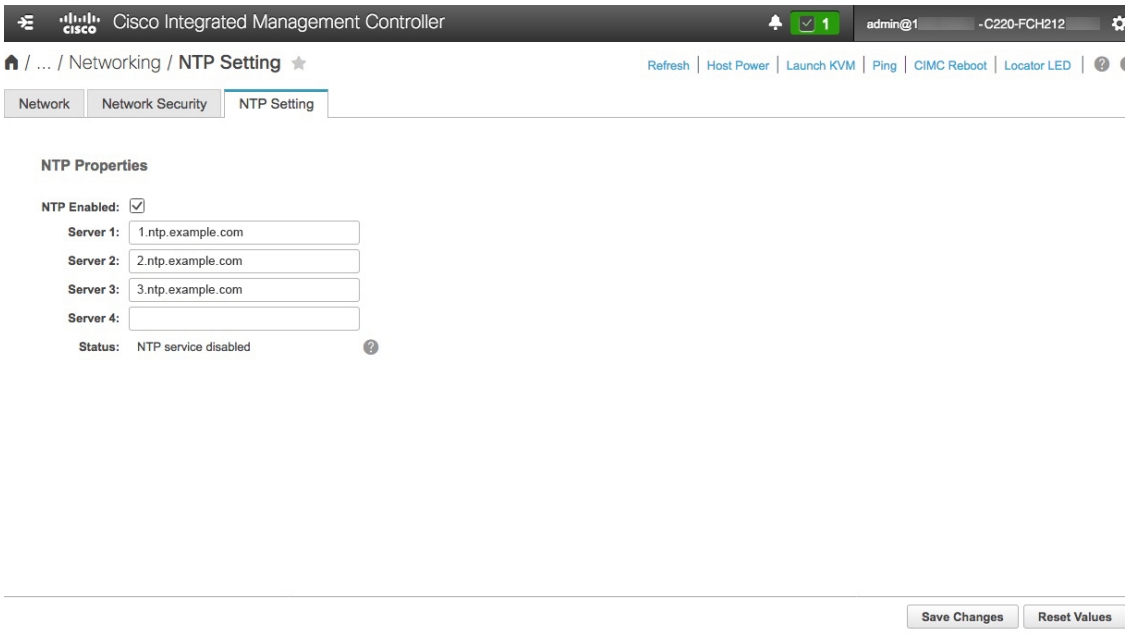



단계 **2** 다음과 같이 네트워크를 관리하는 데 사용하는 NTP(Network Time Protocol) 서버와 어플라이언스 하드웨어를 동기화합니다.

a) 섀시 요약 창이 표시된 상태에서 아이콘을 클릭하여 CIMC 메뉴를 표시합니다.

b) CIMC 메뉴에서 **Admin(**관리자**)** > **Networking(**네트워킹**)** > **NTP Setting(NTP** 설정**)**을 선택합니다. CIMC에서는 **NTP Setting(NTP** 설정**)** 탭을 표시합니다.

c) 아래의 예에 나와 있는 것처럼 **NTP Enabled(NTP** 활성화됨**)** 상자가 선택되었는지 확인한 다음, 4개의 **Server(**서버**)** 필드에 최대 4개의 NTP 서버 호스트 이름 또는 주소를 입력합니다.

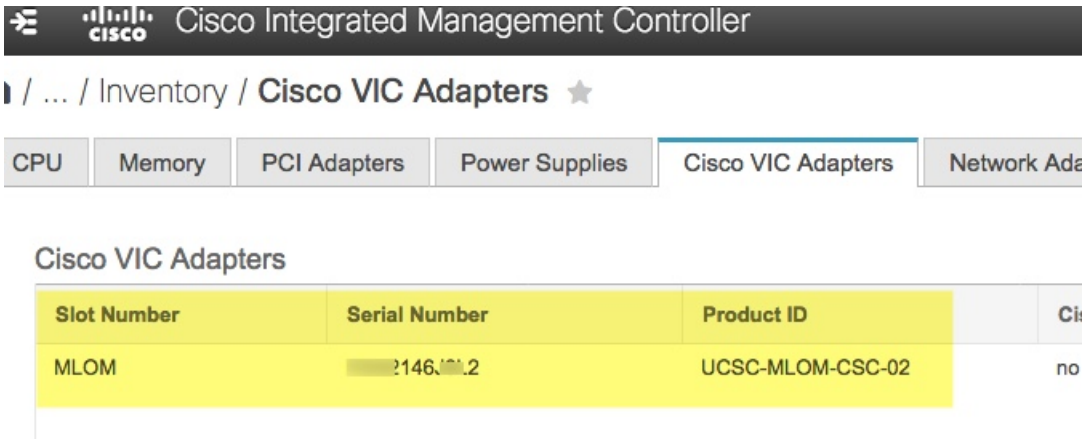


d) 모두 마치면 **Save Changes(**변경 사항 저장**)**를 클릭합니다. CIMC에서는 항목을 검증한 다음, 어플라이언스 하드웨어의 시간을 NTP 서버의 시간과 동기화하기 시작합니다.

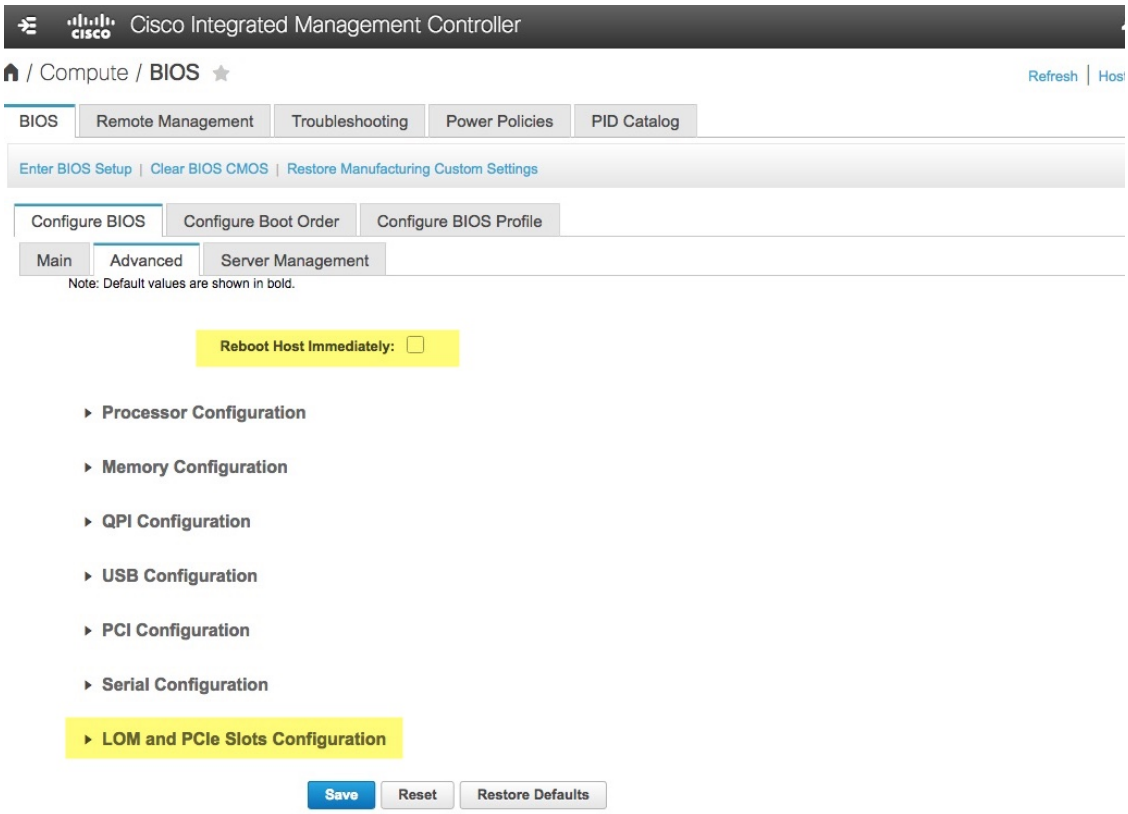
단계 **3** 그런 다음, 다음과 같이 높은 처리량을 지원하도록 어플라이언스 NIC가 구성되었는지 확인합니다.

a) 필요한 경우, ☰ 아이콘을 클릭하여 CIMC 메뉴를 표시합니다.

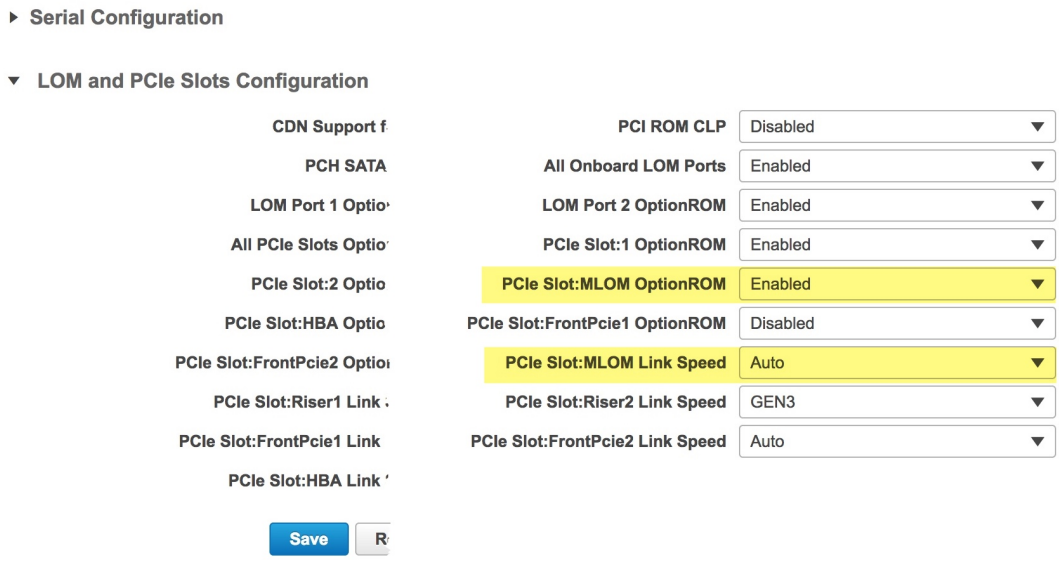
b) CIMC 메뉴에서 **Chassis(**섀시**)** > **Inventory(**인벤토리**)** > **Cisco VIC Adapters(Cisco VIC** 어댑터**)**를 선택합니다. 아래와 같이 MLOM 슬롯에 대해 제품 ID인 "UCSC-MLOM-CSC-02"가 나열되는지 확인합니다.




c) ☰ > **Compute(**컴퓨팅**)** > **BIOS** > **Configure BIOS(BIOS** 구성**)** > **Advanced(**고급**)**를 선택합니다. **Reboot Host Immediately(**호스트 즉시 리부팅**)** 체크 박스가 선택 취소되었는지 확인하고 **LOM and PCIe Slots Configuration(LOM** 및 **PCIe** 슬롯 구성**)** 드롭다운의 위치를 기록해 둡니다.

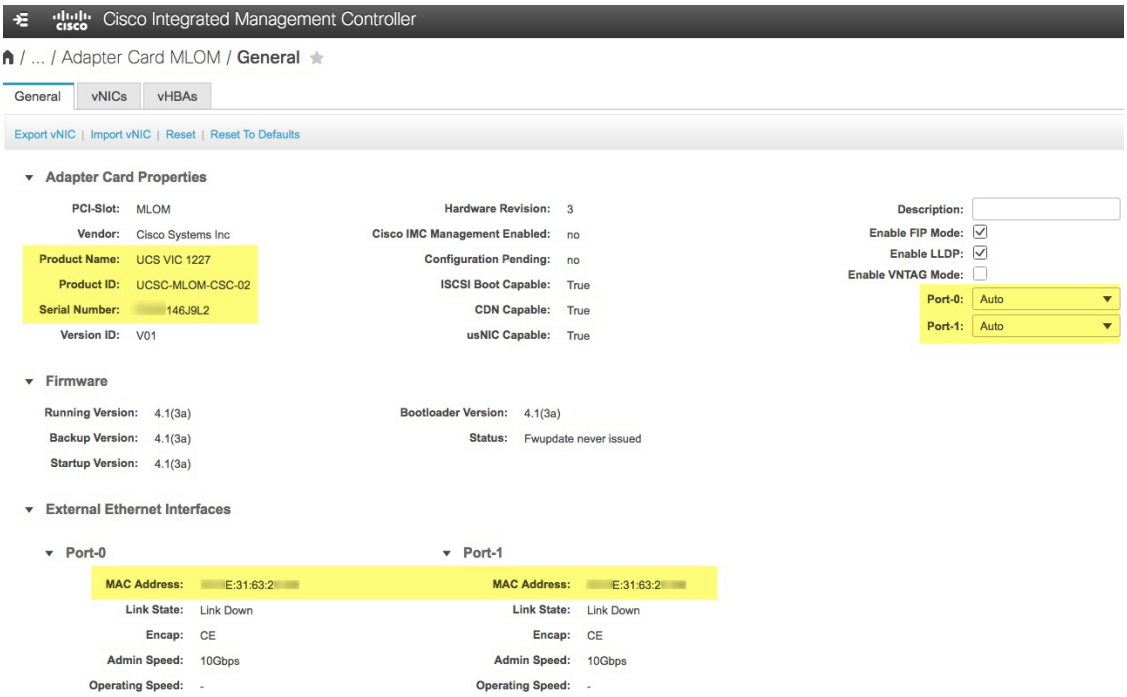



d) **LOM and PCIe Slots Configuration(LOM** 및 **PCIe** 슬롯 구성**)**을 선택합니다. 그런 다음 드롭다운 선택기를 사용하여 **PCIe Slot: MLOM OptionROM(PCIe** 슬롯**: MLOM OptionROM)**을 **Enabled(**활성화됨**)**로 설정하고 **PCIe Slot: MLOM Link Speed(PCIe** 슬롯**: MLOM** 링크 속도**)**를 **Auto(**자동**)**로 설정합니다.



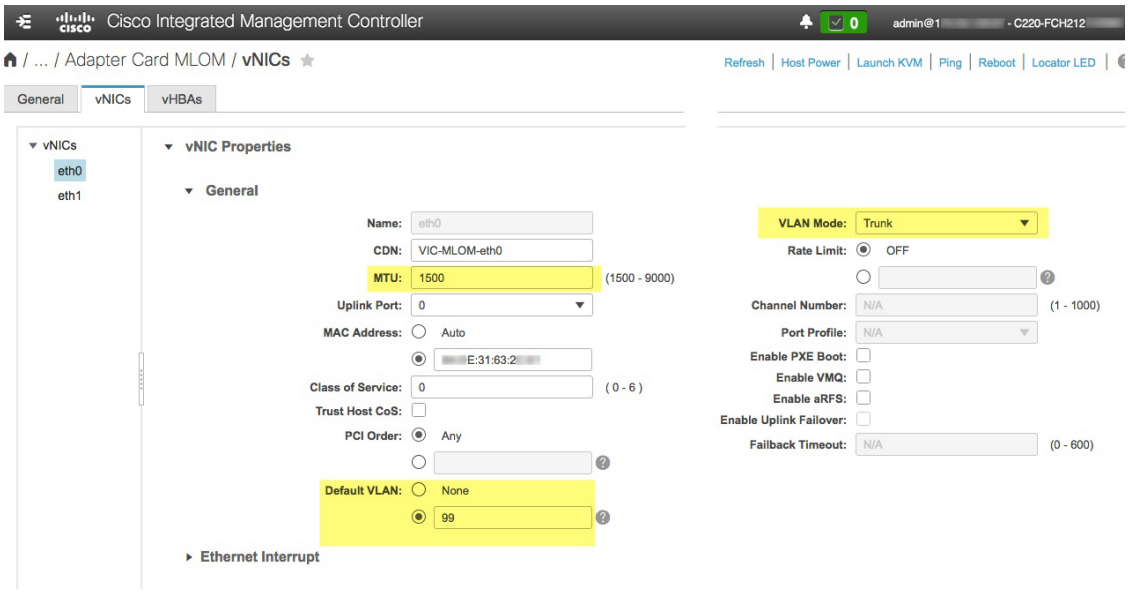

e) **Save(**저장**)**를 클릭합니다. 호스트를 리부팅하라는 프롬프트가 나타납니다. 리부팅하는 대신 **Cancel(**취소**)**을 클릭하고 계속 진행합니다.

f) > **Networking**(네트워킹) > **Adapter Card MLOM**(어댑터 카드 **MLOM**) > **General**(일반)을 선택합니다. **Port-0** 및 **Port-1**의 MAC 주소를 기록해 둡니다(페이지 하단에 있는 외부 이더넷 인터페이스 섹션에 표시됨). **Adapter Card Properties**(어댑터 카드 속성) 섹션에서 **Port-0** 및 **Port-1** 옆의 드롭다운 선택기를 사용하여 아래에 나와 있는 것처럼 두 포트의 속도를 모두 **Auto**(자동)로 설정합니다. 그런 다음 **Save Changes**(변경 사항 저장)를 클릭합니다.




g) **vNICs(vNIC)** 탭을 클릭하고 **vNICs(vNIC)** 드롭다운에서 **eth0**을 선택합니다. 선택기 및 필드를 사용하여 **eth0**에 대해 다음과 같은 값을 설정합니다.

- **VLAN Mode(VLAN 모드): Trunk(트렁크)**
- **MTU: 1500**
- **Default VLAN(기본 VLAN): 99**("99"는 하나의 예시일 뿐입니다. 어플라이언스 및 해당 스위치에서 사용할 기본 VLAN을 입력해야 합니다.)




팁 1500은 최소 MTU 크기입니다. 더 큰 값(최대 9000)을 입력하여 10Gbps 포트에 대한 처리량을 높일 수 있습니다.

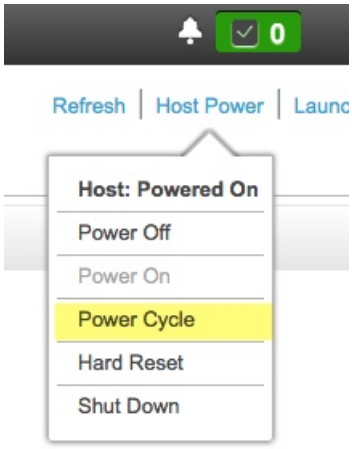
h) **Save Changes(**변경 사항 저장**)**를 클릭합니다. 호스트를 다시 리부팅하라는 프롬프트가 나타납니다. 리부팅하는 대신 작업을 계속하려면 **Cancel(**취소**)**을 클릭합니다.

i) **vNICs(vNIC)** 드롭다운에서 **eth1**을 선택합니다. 드롭다운 선택기를 사용하여 위의 **eth0**에 대해 설정한 값과 동일한 값을 **eth1**에 대해 설정합니다.

j) 모두 마쳤으면 **Save Changes(**변경 사항 저장**)**를 클릭합니다. 호스트를 리부팅하라는 프롬프트가 나타납니다. 이번에는 **OK(**확인**)**를 클릭하여 어플라이언스를 리부팅합니다.

k) 어플라이언스 리부팅이 완료되면 CIMC GUI에 다시 로그인합니다. > **Networking(**네트워킹**)** > **Adapter Card MLOM(**어댑터 카드 **MLOM)** > **General(**일반**)** > **vNICs(vNIC)**를 선택합니다. 이전에 설정한 vNIC MAC 주소와 MTU, VLAN 및 VLAN 모드 파라미터가 정확한지 확인합니다.

l) 작업이 완료되면 오른쪽 상단에 있는 **Host Power(**호스트 전원**)** 메뉴를 클릭하고 **Power Cycle(**전원 껐다가 켜기**)**을 선택합니다. 그리고 **OK(**확인**)**를 클릭합니다.



단계 **4** 그런 다음, 다음과 같이 어플라이언스의 높은 처리량 설정과 일치하도록 스위치를 재구성합니다.

a) SSH(Secure Shell) 클라이언트를 사용하여 구성할 스위치에 로그인하고 스위치 프롬프트에서 EXEC 모드를 시작합니다.

b) 스위치 포트를 구성하려면 다음과 같은 일련의 명령을 입력합니다.

```
MySwitch#Config terminal
MySwitch(config)#interface tengigabitethernet 1/1/3
MySwitch(config-if)#switchport mode trunk
MySwitch(config-if)#switchport trunk allowed vlan 99
MySwitch(config-if)#speed auto
MySwitch(config-if)#duplex full
MySwitch(config-if)#mtu 1500
MySwitch(config-if)#no shut
MySwitch(config-if)#end
MySwitch(config)#copy running-config startup-config
```

이러한 명령은 예시일 뿐입니다. 위에서 어플라이언스 NIC를 구성할 때 입력한 것과 동일한 VLAN ID 및 MTU 값을 사용합니다. 링크 속도, 이중 및 MTU에 대한 명령 값은 예시 스위치의 기본값이므로 기본값을 변경한 경우에만 해당 값을 입력해야 합니다. 어플라이언스 NIC와 마찬가지로 처리량을 높이기 위해 MTU를 최대 9000까지 설정할 수도 있습니다.

c) `show interface tengigabitethernet` *portID* 명령을 실행한 다음, 포트가 연결되어 있으며 실행 중인지, 명령 출력에 올바른 MTU, 이중 및 링크 유형 설정이 있는지 확인합니다. 예를 들면 다음과 같습니다.

```
MySwitch#show interface tengigabitethernet 1/1/3
TenGigabitEthernet1/1/3 is up, line protocol is up (connected)
  Hardware is Ten Gigabit Ethernet, address is XXXe.310.8000 (bia XXX.310.8000)
  MTU 1500 bytes, BW 10000000 Kbit/sec, DLY 10 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive not set
  Full-duplex, 10GB/s, link type is auto, media type is SFP-10Gbase-SR
```

d) `show run interface tengigabitethernet` *portID* 명령을 실행하여 VIC 1227 포트의 케이블이 연결된 스위치 포트를 구성합니다. 예를 들면 다음과 같습니다.

```
MySwitch#show run interface tengigabitethernet 1/1/3
Building configuration...
Current configuration : 129 bytes
! interface TenGigabitEthernet1/1/3
 switchport trunk allowed vlan 99
 switchport mode trunk
 ip device tracking maximum 10
end

MySwitch#
```

e) `how mac address-table interface tengigabitethernet` *portID* 명령을 실행하고 명령 출력에서 MAC 주소를 확인합니다. 예를 들면 다음과 같습니다.

```
MySwitch#show mac address-table interface tengigabitethernet 1/1/3
          Mac Address Table
-------------------------------------------
Vlan    Mac Address       Type        Ports
----    -----------       ----        -----
99      XXXe.3161.1000    DYNAMIC     Te1/1/3
Total Mac Addresses for this criterion: 1

MySwitch#
```

단계 **5** 마지막으로, 다음과 같이 10Gbps 어플라이언스 포트에 연결된 스위치가 크기가 큰 802.1p 프레임을 지원하도록 구성합니다.

a) 아직 이 작업을 수행하지 않은 경우, SSH(Secure Shell) 클라이언트를 사용하여 구성할 스위치에 로그인하고 스위치 프롬프트에서 EXEC 모드를 시작합니다.

b) 802.1P 프레임을 지원하도록 스위치 포트를 구성하려면 다음과 같은 일련의 명령을 입력합니다.

```
MySwitch#Config terminal
MySwitch(config)#interface tengigabitethernet 1/1/3
MySwitch(config-if)#switchport voice vlan dot1p
MySwitch(config-if)#no shut
MySwitch(config-if)#end
MySwitch(config)#copy running-config startup-config
```

c) `show run interface tengigabitethernet` *`portID`* 명령을 실행하고 포트에 올바른 `voice vlan dot1p` 설정이 있는지 명령 출력에서 확인합니다. 예를 들면 다음과 같습니다.

```
MySwitch#show run interface tengigabitEthernet 1/1/3
Building configuration...

Current configuration : 62 bytes
!
interface tengigabitethernet1/1/3
switchport mode trunk
switchport voice vlan dot1p
MySwitch#end
```

---

다음에 수행할 작업

처음 설치된 어플라이언스를 클러스터의 마스터 노드로 구성하여 계속 진행합니다. 마스터 노드 구성을 참조하십시오.

# Cisco DNA Center ISO 이미지 확인

Cisco DNA Center를 구축하기 전에 다운로드한 ISO 이미지가 정품 Cisco 이미지임을 확인하는 것이 좋습니다.

시작하기 전에

이메일 또는 Cisco 지원 팀에 문의하여 Cisco DNA Center ISO 이미지의 위치를 가져옵니다.

---

단계 **1** Cisco에서 지정한 위치에서 Cisco DNA Center ISO 이미지(.iso)를 다운로드합니다.

단계 **2** Cisco에서 지정한 위치에서 시그니처 확인용 Cisco 공개 키(cisco_image_verification_key.pub)를 다운로드합니다.

단계 **3** Cisco에서 지정한 위치에서 ISO 이미지의 보안 해시 알고리즘(SHA512) 체크섬 파일을 다운로드합니다.

단계 **4** 이메일을 통해 Cisco 지원 팀으로부터 ISO 이미지의 시그니처 파일(.sig)을 받거나 안전한 Cisco 웹 사이트(제공되는 경우)에서 이를 다운로드합니다.

단계 **5** (선택 사항) SHA 검증을 수행하여 ISO 이미지가 부분 다운로드로 손상되었는지 여부를 확인합니다.

(운영 체제에 따라) 다음 명령 중 하나를 실행합니다.

- Linux 시스템의 경우: **sha512sum** *ISO-image-filename*
- Mac 시스템의 경우: **shasum -a 512** *ISO-image-filename*

Microsoft Windows에는 체크섬 유틸리티가 내장되어 있지 않지만, Microsoft의 http://www.microsoft.com/en-us/download/details.aspx?id=11533 링크에서 유틸리티를 설치할 수 있습니다. 위 명령(또는 Microsoft Windows 유틸리티)의 출력을 3단계에서 다운로드한 SHA512 체크섬 파일과 비교합니다. 명령 출력이 일치하지 않을 경우 다시 ISO 이미지를 다운로드하고 명령을 실행합니다. 여전히 출력이 일치하지 않을 경우 Cisco 지원에 문의하십시오.

단계 **6** 시그니처를 통해 ISO 이미지가 Cisco에서 제공한 정품임을 확인합니다.

**openssl dgst -sha512 -verify cisco_image_verification_key.pub -signature** *signature-filename ISO-image-filename*

참고 이 명령은 MAC 및 Linux 환경을 모두 지원합니다. Windows의 경우 OpenSSL을 다운로드하고 설치하지 않았다면(여기에서 사용 가능) 다운로드하여 설치해야 합니다.

ISO 이미지가 정품일 경우 이 명령을 실행하면 **Verified OK**(정상 확인) 메시지가 나타납니다. 이 메시지가 나타나지 않을 경우 ISO 이미지를 설치하지 말고 Cisco 지원에 문의하십시오.

단계 **7** Cisco ISO 이미지를 다운로드했는지 확인한 후에는 Cisco DNA Center ISO 이미지가 포함된 부팅 가능한 USB 드라이브를 생성합니다. 부팅 가능 USB 드라이브 생성을 참조하십시오.

# 부팅 가능 USB 드라이브 생성

다음 절차를 완료하여 Cisco DNA Center ISO 이미지를 설치할 수 있는 부팅 가능한 USB 드라이브를 생성합니다.

시작하기 전에

- Cisco DNA Center ISO 이미지의 복사본을 다운로드하고 확인합니다. Cisco DNA Center ISO 이미지 확인을 참조하십시오.
- 사용 중인 USB 플래시 드라이브의 용량이 32GB 이상인지 확인합니다.

단계 **1** 노트북 또는 데스크톱에서 부팅 가능한 USB 드라이브를 생성할 수 있는 오픈소스 프리웨어 유틸리티인 Etcher(1.3.1 이상 버전)를 다운로드하여 설치합니다.

현재 Etcher의 Linux, macOS 및 Windows 버전을 사용할 수 있습니다. https://www.balena.io/etcher/에서 복사본을 다운로드할 수 있습니다.

참고 Etcher의 Windows 버전은 이전 버전의 Windows와 알려진 호환성 문제가 있으므로 Windows 10을 실행 중인 시스템에서만 사용하십시오.

단계 **2** Etcher를 설치한 시스템에서 USB 드라이브를 연결한 다음, Etcher를 시작합니다.

단계 **3** 창의 오른쪽 상단에 있는 기어 아이콘을 클릭하고 다음과 같은 Etcher 설정이 설정되었는지 확인합니다.

- 성공 시 자동 마운트 해제
- 성공 시 쓰기 검증

단계 **4** **Back(**뒤로**)**을 클릭하여 기본 창으로 돌아갑니다.

단계 **5** **Select Image(**이미지 선택**)**를 클릭합니다.

단계 **6** 이전에 다운로드한 Cisco DNA Center ISO 이미지로 이동하여 선택한 다음, **Open(**열기**)**을 클릭합니다.

연결된 USB 드라이브의 이름이 드라이브 아이콘 아래에 나열되어야 합니다. 그렇지 않은 경우에는 다음 작업을 수행하십시오.

1. **Select drive(**드라이브 선택**)**를 클릭합니다.
2. 올바른 USB 드라이브의 라디오 버튼을 클릭한 다음, **Continue(**계속**)**를 클릭합니다.

단계 **7** **Flash!(**플래시**!)**를 클릭하여 USB 드라이브에 ISO 이미지를 복사합니다.

Etcher에서 USB 드라이브를 Cisco DNA Center ISO 이미지가 설치된 부팅 가능한 드라이브로 구성합니다.

# 어플라이언스 이미지 재설치

백업에서 복구하거나 클러스터 링크 구성을 변경하는 등 Cisco DNA Center 어플라이언스를 이미지로 다시 설치해야 하는 상황이 발생할 수 있습니다. 이 작업을 위해서는 다음 절차를 완료하십시오.

단계 **1** Cisco DNA Center ISO 이미지를 다운로드하고 정품 Cisco 이미지인지 확인합니다.

"Cisco DNA Center IOS 이미지 확인"을 참조하십시오.

단계 **2** Cisco DNA Center ISO 이미지가 포함된 부팅 가능한 USB 드라이브를 생성합니다.

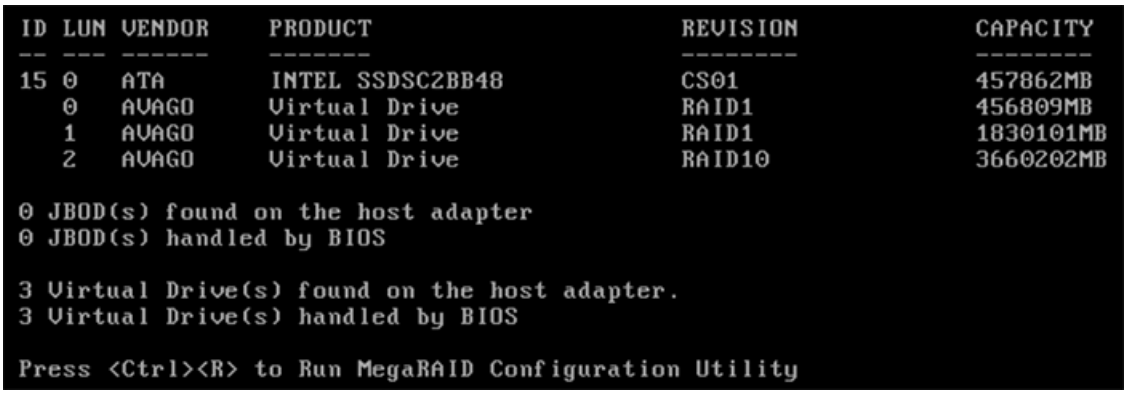
"부팅 가능한 USB 드라이브 생성"을 참조하십시오.

단계 **3** 어플라이언스의 RAID 컨트롤러에서 관리하는 3개의 가상 드라이브를 다시 초기화합니다.

a) Cisco IMC에 로그인하여 KVM 세션을 시작합니다.
b) 다음 메뉴 옵션 중 하나를 선택하여 어플라이언스를 켜거나 껐다가 켭니다.

- **Power(**전원**)** > **Power On System(**시스템 켜기**)**
- **Power(**전원**)** > **Power Cycle System (cold boot)(**시스템 껐다가 켜기**(**콜드 부트**))**

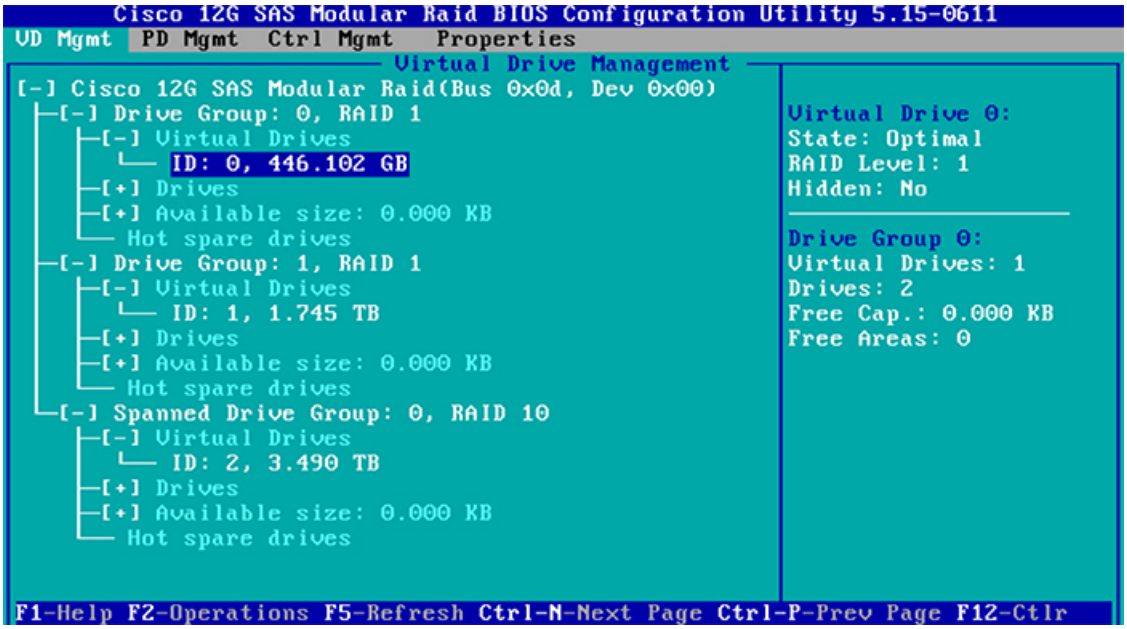
어플라이언스를 리부팅하면 어플라이언스의 모든 드라이브(물리적 및 가상 모두)가 나열된 화면이 표시됩니다.




c) 이 화면이 표시되면 바로 **Ctrl** + **R** 키를 눌러 MegaRAID Configuration Utility를 실행합니다.

너무 오래 기다리면 이 화면이 사라집니다. 이 화면으로 돌아가려면 KVM 메뉴에서 **Power(**전원**)** > **Reset System(warm boot)(**시스템 리셋**(**웜 부팅**))**을 선택하여 어플라이언스를 리부팅합니다.

d) 드라이브 항목(`ID: 0, 446.102GB` 등)을 선택하고 **F2** 키를 누릅니다.




이렇게 하면 드라이브의 **Advanced Properties(**고급 속성**)** 화면이 열립니다.

e) 결과 메뉴에서 **Initialization(**초기화**)** > **Fast Initialization(**빠른 초기화**)**을 선택합니다.

f) 어플라이언스의 다른 가상 드라이브에 대해 3b~3e단계를 반복합니다.

단계 **4** 어플라이언스에 Cisco DNA Center를 다시 설치합니다.

"Cisco DNA Center IOS 이미지 설치"를 참조하십시오.

# Cisco DNA Center ISO 이미지 설치

다음 절차를 수행하여 Cisco DNA Center ISO 이미지를 어플라이언스에 설치합니다.

시작하기 전에

- Cisco DNA Center ISO 이미지를 설치할 부팅 가능한 USB 드라이브를 생성합니다. "부팅 가능 USB 드라이브 생성"을 참조하십시오.
- Cisco DNA Center의 다른 버전이 이미 어플라이언스에 설치되어 있는 경우 "어플라이언스를 이미지로 다시 설치"에 설명된 절차를 완료합니다.

---

단계 **1** Cisco DNA Center ISO 이미지가 포함된 부팅 가능한 USB 드라이브를 어플라이언스에 연결합니다.

단계 **2** CIMC에 로그인하여 KVM 세션을 시작합니다.

단계 **3** 다음과 같이 어플라이언스의 전원을 켜거나 껐다가 켭니다.

- 어플라이언스를 현재 실행하고 있지 않은 경우 **Power(**전원**)** > **Power On System(**시스템 전원 켜기**)**을 선택합니다.
- 어플라이언스를 이미 실행 중인 경우 **Power(**전원**)** > **Power Cycle System (cold boot)(**시스템 껐다가 켜기**(**콜드 부트**))**을 선택합니다.

단계 **4** 결과 팝업 창에서 **Yes(**예**)**를 클릭하여 서버 제어 작업을 실행할 것이라는 점을 확인합니다.

단계 **5** Cisco 로고가 표시되면 KVM 메뉴에서 **F6** 키를 누르거나 **Macros(**매크로**)** > **User Defined Macros(**사용자 정의 매크로**)** > **F6** 키를 선택합니다.

부팅 디바이스 선택 메뉴가 나타납니다.

단계 **6** USB 드라이브를 선택한 다음, **Enter** 키를 누릅니다.

단계 **7** **GNU GRUB** 부팅 로더 창에서 **Manufacture Cisco DNA appliance(**제조사 **Cisco DNA** 어플라이언스**)**를 선택한 다음, **Enter** 키를 누릅니다.

참고 30초 이내에 선택하지 않으면 부팅 로더에서 자동으로 Maglev 설치 프로그램을 부팅합니다. 그 전에 선택한 사항을 확인하십시오.

Cisco DNA Center ISO 이미지 설치가 완료되면 설치 프로그램이 리부팅되고 Maglev 구성 마법사가 열립니다.

---

# 마스터 노드 구성

처음 설치된 어플라이언스를 마스터 노드로 구성하려면 다음 단계를 수행합니다. 첫 번째 어플라이언스가 독립형으로 작동하든, 아니면 클러스터의 일부로 작동하든 해당 어플라이언스는 항상 마스터 노드로 구성해야 합니다.

이미 마스터 노드가 있는 기존 클러스터에 대한 추가 기능 노드로 설치된 어플라이언스를 구성하는 경우에는 대신 추가 기능 노드 구성의 단계를 수행합니다.

중요 클러스터의 각 어플라이언스에 대해 해당 인터페이스 중 하나에서만 DNS 서버를 구성합니다. 여러 인터페이스에서 DNS 서버를 구성하는 경우 문제가 발생할 수 있습니다.

시작하기 전에

확인:

- 필수 서브넷 및 추가 IP 주소과 필수 구성 정보에서 요구하는 모든 정보를 수집했는지 확인합니다.
- 어플라이언스 설치 워크플로에 설명된 대로 첫 번째 어플라이언스를 설치했는지 확인합니다.
- CIMC에 대한 브라우저 액세스 활성화에 설명된 대로 마스터 노드에서 CIMC 브라우저 액세스를 구성했는지 확인합니다.
- 사전 검사 실행에 설명된 대로 마스터 노드 어플라이언스의 포트와 그에 의해 사용되는 스위치가 올바르게 구성되었는지 확인합니다.
- CIMC 및 Cisco DNA Center와 호환 가능한 브라우저를 사용하고 있는지 확인합니다. 호환되는 브라우저 목록은 설치 중인 Cisco DNA Center의 버전에 대한 릴리스 노트를 참조하십시오.
- 다음 절차의 8단계에서 지정하는 Cisco DNA Center와 DNS 서버 간의 방화벽에서 ICMP를 활성화했는지 확인합니다. Maglev 구성 마법사에서는 Ping을 사용하여 사용자가 지정하는 DNS 서버를 확인합니다. Cisco DNA Center와 DNS 서버 간에 방화벽이 있고 해당 방화벽에서 ICMP가 활성화되어 있지 않으면 이 ping을 차단할 수 있습니다. 그러면 마법사를 완료할 수 없게 됩니다.

단계 **1** 브라우저에서 CIMC GUI 구성 시 설정한 CIMC IP 주소로 이동하고 CIMC GUI에 CIMC 사용자로 로그인합니다(CIMC에 대한 브라우저 액세스 활성화 참조).

로그인이 완료되면 다음 그림과 같이 어플라이언스에 **Cisco Integrated Management Controller** 새시 요약 창이 표시되고 아래에 나와 있는 것과 같이 오른쪽 상단에 파란색 링크 메뉴가 표시됩니다.

단계 **2** 파란색 링크 메뉴에서 **Launch KVM(KVM 실행)**을 선택한 다음, **Java based KVM(Java 기반 KVM)** 또는 **HTML based KVM(HTML 기반 KVM)**을 선택합니다. Java 기반 KVM을 선택하는 경우 KVM 콘솔을 해당 콘솔 창에서

확인하려면 브라우저 또는 파일 관리자에서 Java 시작 파일을 실행해야 합니다. HMTL 기반 KVM을 선택하는 경우에는 KVM 콘솔이 별도의 브라우저 창 또는 탭에서 자동으로 실행됩니다.

선택하는 KVM 유형과 관계없이 KVM 콘솔을 사용하여 구성의 진행 상황을 모니터링하고 Maglev 구성 마법사 프롬프트에 응답합니다.

단계 **3** KVM이 표시되면 다음 선택 사항 중 하나를 수행하여 어플라이언스를 리부팅합니다.

a) 기본 CIMC GUI 브라우저 창에서 **Host Power(**호스트 전원**)** > **Power Cycle(**전원 껐다가 켜기**)**을 선택합니다. 그런 다음 KVM 콘솔로 전환하여 계속 진행합니다.

b) KVM 콘솔에서 **Power(**전원**)** > **Power Cycle System (cold boot)(**시스템 껐다가 켜기**(**콜드 부트**))**을 선택합니다.

어플라이언스를 리부팅할 것인지 선택하라는 메시지가 표시되면 **OK(**확인**)**를 클릭합니다.

리부팅 메시지가 표시된 후 KVM 콘솔에는 아래에 나와 있는 Maglev 구성 마법사 시작 화면이 표시됩니다.

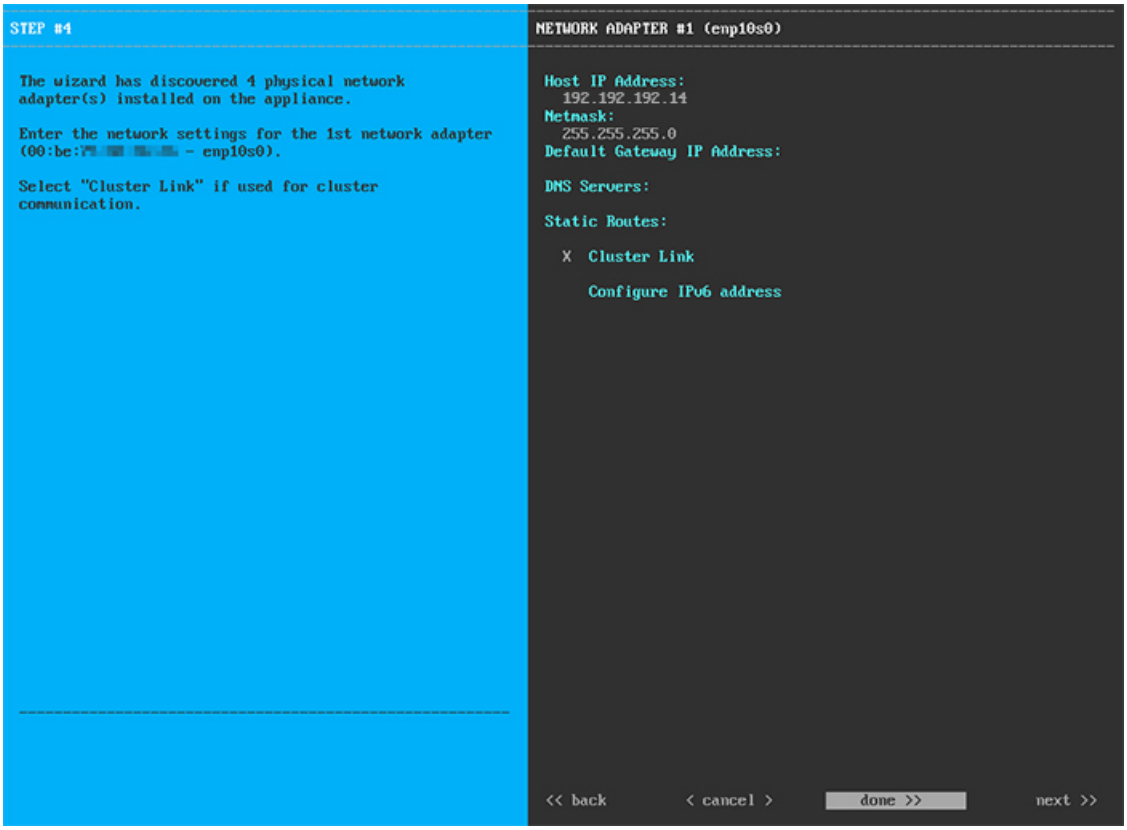
단계 **4** 마스터 노드 구성을 시작하려면 **Start a DNA-C cluster(DNA-C** 클러스터 시작**)**를 선택합니다.

마법사에서는 어플라이언스의 모든 포트를 검색하여 별도의 화면에 하나씩 다음과 같은 순서로 표시합니다.

1. 10Gbps 클러스터 포트(포트 2, enp10s0, 네트워크 어댑터 #1)
2. 1Gbps Cisco DNA Center GUI 포트(1, enp1s0f0, 네트워크 어댑터 #2)
3. 1Gbps 클라우드 포트(2, enp1s0f1, 네트워크 어댑터 #3)
4. 10Gbps 엔터프라이즈 포트(포트 1, enp9s0, 네트워크 어댑터 #4)

참고 마법사에서 구성 시 10Gbps 포트 중 하나 또는 둘 다를 표시하지 못하는 경우에는 이러한 포트가 작동하지 않거나 비활성화된 것일 수 있습니다. 이러한 10Gbps 포트는 Cisco DNA Center 기능에 필요합니다. 이러한 포트가 작동하지 않는 것을 발견하면 **cancel(취소)**을 선택하여 즉시 구성을 종료합니다. 구성을 다시 시작하거나 Cisco TAC(Technical Assistance Center)에 연결하기 전에 사전 검사 실행에서 제공된 모든 단계를 완료했는지 확인하십시오.

단계 **5** 마법사에서는 10Gbps 클러스터 포트(포트 2, enp10s0)를 먼저 검색하여 **NETWORK ADAPTER #1(**네트워크 어댑터 **#1)**로 표시합니다. 인터페이스 케이블 연결에 설명된 것처럼 이 포트는 어플라이언스를 클러스터에 연결하는 데 사용되므로 이 목적에 적합한 호스트 IP 주소, 넷마스크 및 기타 값을 적용합니다(입력할 값은 필수 서브넷 및 추가 IP 주소, 필수 구성 정보 참조).




아래 표에 나와 있는 것처럼 **NETWORK ADAPTER #1(**네트워크 어댑터 **#1)**에 대한 구성 값을 입력합니다.

표 ***22:*** 네트워크 어댑터 ***#1: 10Gbps*** 클러스터 포트***(enp10s0)***에 대한 마스터 노드 항목

| | |
|---|---|
| **Host IP address(**호스트 **IP** 주소**)** | 클러스터 포트의 IP 주소를 입력합니다. 이는 필수 항목입니다. 나중에 클러스터 포트의 주소를 변경할 수 없습니다. |
| **Netmask** | 포트의 IP 주소에 대한 넷마스크를 입력합니다. 이는 필수 값입니다. |
| **Default Gateway IP address(**기본 게이트웨이 **IP** 주소**)** | 포트에 사용할 기본 게이트웨이 IP 주소를 입력합니다. 이는 일반적으로 엔터프라이즈 포트에만 필요합니다. |

| | |
|---|---|
| **DNS** 서버 | 기본 설정된 DNS 서버의 IP 주소를 입력합니다. 여러 DNS 서버를 입력하는 경우 목록에 있는 IP 주소를 공백으로 구분합니다. |
| **Static Routes(**고정 경로**)** | <network>/<netmask>/<gateway>와 같은 형식으로 하나 이상의 정적 경로를 공백으로 구분하여 입력합니다. 이는 일반적으로 GUI 포트에만 필요합니다. |
| **Cluster Link(**클러스터 링크**)** | 이 포트를 클러스터에 대한 링크로 지정하려면 체크 박스를 선택합니다. 이는 클러스터 포트에만 필요합니다. |
| **Configure IPv6 Address(IPv6** 주소 구성**)** | 이후 사용을 위해 예약됩니다. 이 필드는 비워둡니다. |

구성 값을 입력했으면 **next>>(**다음>>**)**를 입력하여 계속 진행합니다. **next>>(**다음>>**)**를 입력하고 나면 마법사에서 입력한 값을 검증하고 잘못된 값이 있는 경우 오류 메시지를 표시합니다. 오류 메시지가 표시되면 입력한 값이 정확한지 확인한 다음, 다시 입력합니다. 필요한 경우 **<<back(<<**뒤로**)**을 선택하여 다시 입력합니다.

단계 **6** 입력한 클러스터 포트 값의 검증이 완료되면 마법사에서 1Gbps Cisco DNA Center GUI 포트(1, enp1s0f0)를 **NETWORK ADAPTER #2(**네트워크 어댑터 **#2)**로 표시합니다. 인터페이스 케이블 연결에에 설명된 것처럼 이 포트는 관리 네트워크에서 Cisco DNA Center GUI에 액세스하는 데 사용됩니다. 이 목적에 적합한 호스트 IP 주소, 넷마스크 및 기타 값을 적용합니다(입력할 값은 필수 서브넷 및 추가 IP 주소, 필수 구성 정보 참조).

아래 표에 나와 있는 것처럼 **NETWORK ADAPTER #2(**네트워크 어댑터 **#2)**에 대한 구성 값을 입력합니다.

표 *23:* 네트워크 어댑터 *#2: 1Gbps GUI* 포트*(enp1s0f0)*에 대한 마스터 노드 항목

| | |
|---|---|
| **Host IP address(**호스트 **IP** 주소**)** | 1Gpbs GUI 포트의 IP 주소를 입력합니다. 이는 필수 값입니다. |
| **Netmask** | 포트의 IP 주소에 대한 넷마스크를 입력합니다. 이는 필수 값입니다. |
| **Default Gateway IP address(**기본 게이트웨이 **IP** 주소**)** | 포트에 사용할 기본 게이트웨이 IP 주소를 입력합니다. 이는 일반적으로 엔터프라이즈 포트에만 필요합니다. |
| **DNS** 서버 | 기본 설정된 DNS 서버의 IP 주소를 입력합니다. 여러 DNS 서버를 입력하는 경우 목록에 있는 IP 주소를 공백으로 구분합니다.<br>참고 NTP의 경우, Cisco DNA Center 및 NTP 서버 간에 포트 121(UDP)이 열려 있는지 확인합니다. |
| **Static Routes(**고정 경로**)** | 다음 형식으로 하나 이상의 정적 경로를 공백으로 구분하여 입력합니다. <network>/<netmask>/<gateway>. |
| 클러스터 링크 | 이 필드는 비워둡니다. 이는 클러스터 포트에만 필요합니다. |
| **IPv6** 주소 구성 | 이후 사용을 위해 예약됩니다. 이 필드는 비워둡니다. |

작업을 완료하면 **next>>(**다음**>>)**를 입력하여 계속 진행합니다. 이전 화면에서 수행한 것처럼 검증 오류를 수정합니다.

단계 **7** 입력한 Cisco DNA Center GUI 포트 값의 검증이 완료되면 마법사에서는 1Gbps 클라우드 포트(2, enp1s0f1)를 **NETWORK ADAPTER #3(**네트워크 어댑터 **#3)**으로 표시합니다. 인터페이스 케이블 연결에 설명된 것처럼, 이는 10Gbps 엔터프라이즈 포트(포트 1, enp9s0)를 통해 어플라이언스를 인터넷에 연결할 수 없는 경우 그렇게 하는 데 사용되는 포트(선택 사항)입니다. 이 목적에 적합한 호스트 IP 주소, 넷마스크 및 기타 값을 적용합니다(필수 서브넷 및 추가 IP 주소 및 필수 구성 정보 참조).

아래 표에 나와 있는 것처럼 **NETWORK ADAPTER #3**(네트워크 어댑터 **#3**)에 대한 구성 값을 입력합니다.

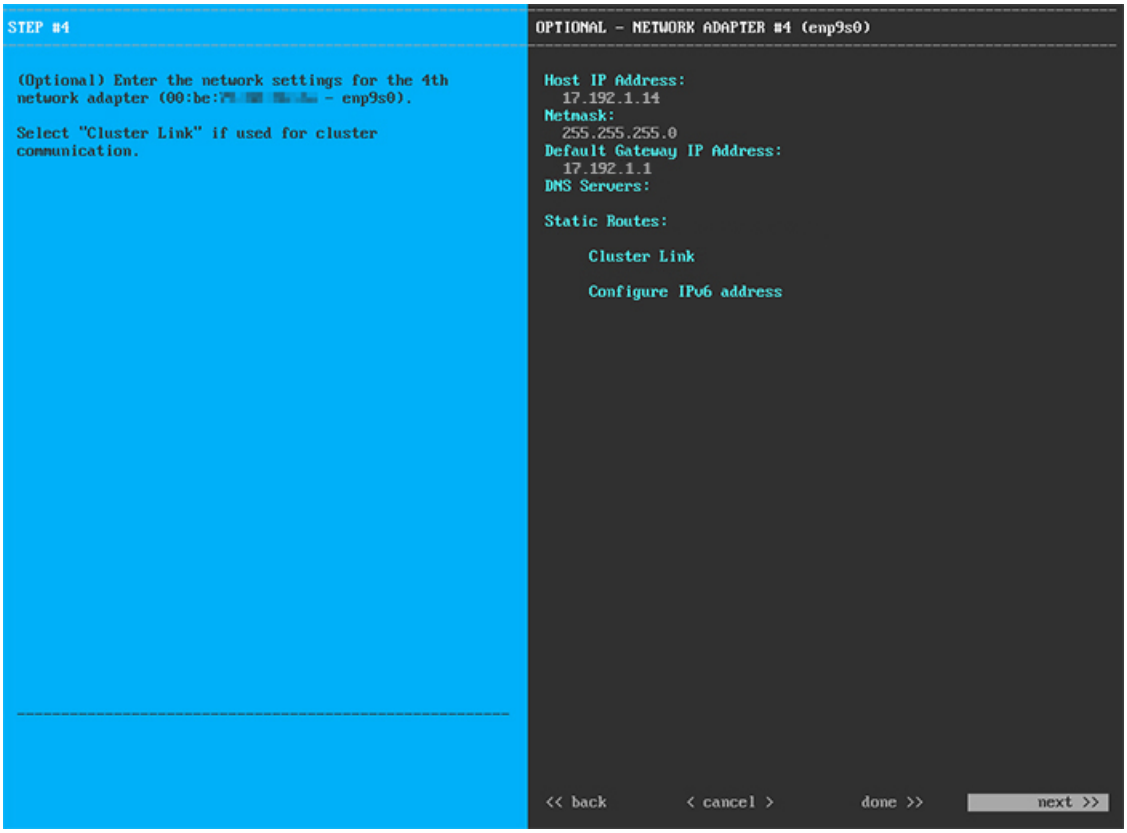
표 ***24:*** 네트워크 어댑터 ***#3: 1Gbps*** 클라우드 포트***(enp1s0f1)***에 대한 마스터 노드 항목

| | |
|---|---|
| **Host IP address**(호스트 **IP** 주소) | 클라우드 포트의 IP 주소를 입력합니다. 이는 인터넷 연결에 클라우드 포트를 사용하는 경우에만 필요합니다. 그렇지 않은 경우에는 비워둘 수 있습니다. |
| **Netmask** | 포트의 IP 주소에 대한 넷마스크를 입력합니다. 이는 IP 주소를 입력하는 경우 필요합니다. |
| **Default Gateway IP address**(기본 게이트웨이 **IP** 주소) | 클라우드 포트에 사용할 기본 게이트웨이 IP 주소를 입력합니다. 이는 일반적으로 엔터프라이즈 포트에만 필요합니다. |
| **DNS** 서버 | 기본 설정된 DNS 서버의 IP 주소를 입력합니다. 여러 DNS 서버를 입력하는 경우 목록에 있는 IP 주소를 공백으로 구분합니다. |
| **Static Routes**(고정 경로) | 다음 형식으로 하나 이상의 정적 경로를 공백으로 구분하여 입력합니다. <network>/<netmask>/<gateway>. 이는 일반적으로 Cisco DNA Center GUI 포트에만 필요합니다. |

| | |
|---|---|
| 클러스터 링크 | 이 필드는 비워둡니다. 이는 클러스터 포트에만 필요합니다. |
| **IPv6** 주소 구성 | 이후 사용을 위해 예약됩니다. 이 필드는 비워둡니다. |

작업을 완료하면 **next>>(**다음>>**)**를 입력하여 계속 진행합니다. 이전 화면에서 수행한 것처럼 유효성 검사 오류를 수정합니다.

단계 **8** 입력한 클라우드 포트 값의 검증이 완료되면 마법사에서는 10Gbps 엔터프라이즈 포트( 포트 1, enp9s0)를 **NETWORK ADAPTER #4(**네트워크 어댑터 **#4)**로 표시합니다. 인터페이스 케이블 연결에 설명된 것처럼, 이는 어플라이언스를 엔터프라이즈 네트워크에 연결하는 데 사용되는 필수 포트입니다. 이 목적에 적합한 호스트 IP 주소, 넷마스크 및 기타 값을 적용합니다(입력할 값은 필수 서브넷 및 추가 IP 주소, 필수 구성 정보 참조).




아래 표에 나와 있는 것처럼 **NETWORK ADAPTER #4(**네트워크 어댑터 **#4)**에 대한 구성 값을 입력합니다.

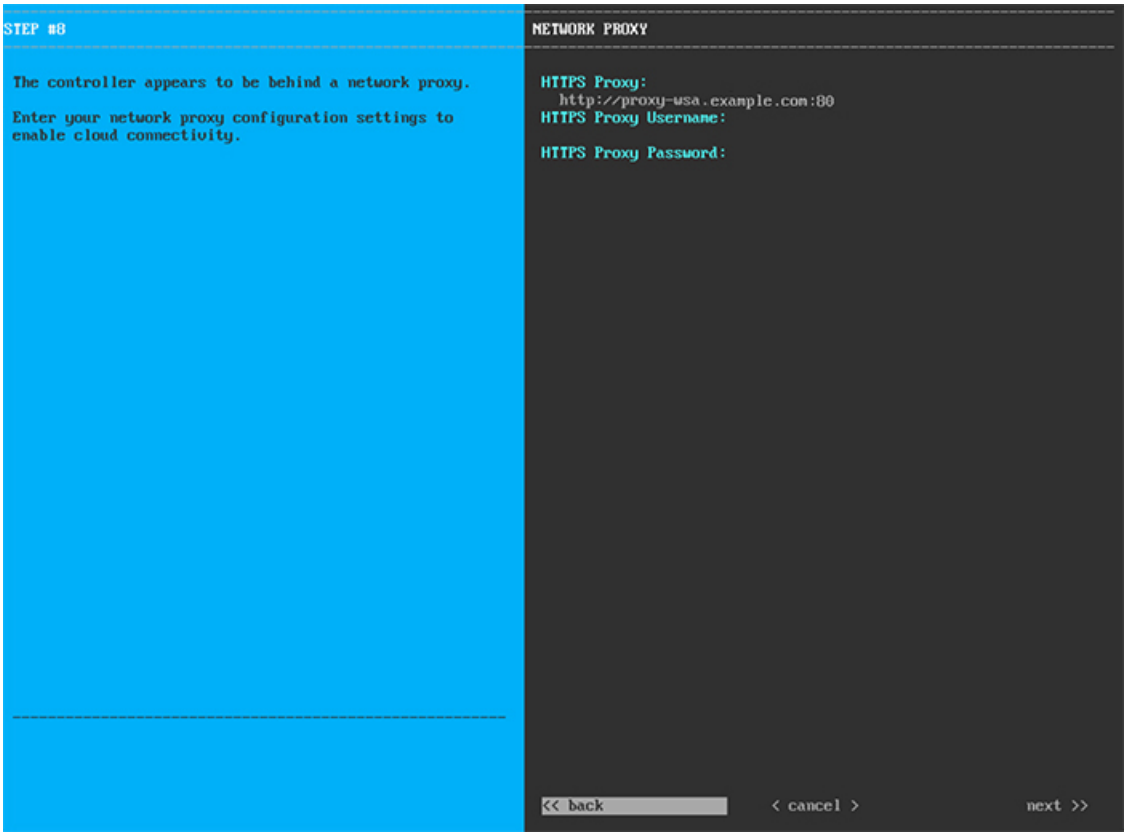
표 ***25:*** 네트워크 어댑터 ***#4: 10Gbps*** 엔터프라이즈 포트***(enp9s0)***에 대한 마스터 노드 항목

| | |
|---|---|
| **Host IP address(**호스트 **IP** 주소**)** | 10Gpbs 엔터프라이즈 포트의 IP 주소를 입력합니다. 이는 필수 값입니다. |
| **Netmask** | 포트의 IP 주소에 대한 넷마스크를 입력합니다. 이는 필수 값입니다. |

| | |
|---|---|
| **Default Gateway IP address**(기본 게이트웨이 **IP** 주소) | 포트에 사용할 기본 게이트웨이 IP 주소를 입력합니다. 이는 필수 값입니다. |
| **DNS** 서버 | 기본 설정된 DNS 서버의 IP 주소를 입력합니다. 여러 DNS 서버를 입력하는 경우 목록에 있는 IP 주소를 공백으로 구분합니다. |
| **Static Routes**(고정 경로) | 다음 형식으로 하나 이상의 정적 경로를 공백으로 구분하여 입력합니다. <network>/<netmask>/<gateway>. 이는 일반적으로 Cisco DNA Center GUI 포트에만 필요합니다. |
| 클러스터 링크 | 이 필드는 비워둡니다. 이는 클러스터 포트에만 필요합니다. |
| **IPv6** 주소 구성 | 이후 사용을 위해 예약됩니다. 이 필드는 비워둡니다. |

작업을 완료하면 **next>>**(다음>>)를 입력하여 계속 진행합니다. 이전 화면에서 수행한 것처럼 유효성 검사 오류를 수정합니다. 마법사에서 네트워크 어댑터 구성을 검증하고 적용합니다.

단계 **9** 네트워크 어댑터 구성이 완료되면 마법사에서는 아래에 나와 있는 것처럼 사용 중인 **NETWORK PROXY**(네트워크 프록시)에 대한 구성 값을 입력하라는 프롬프트를 표시합니다.



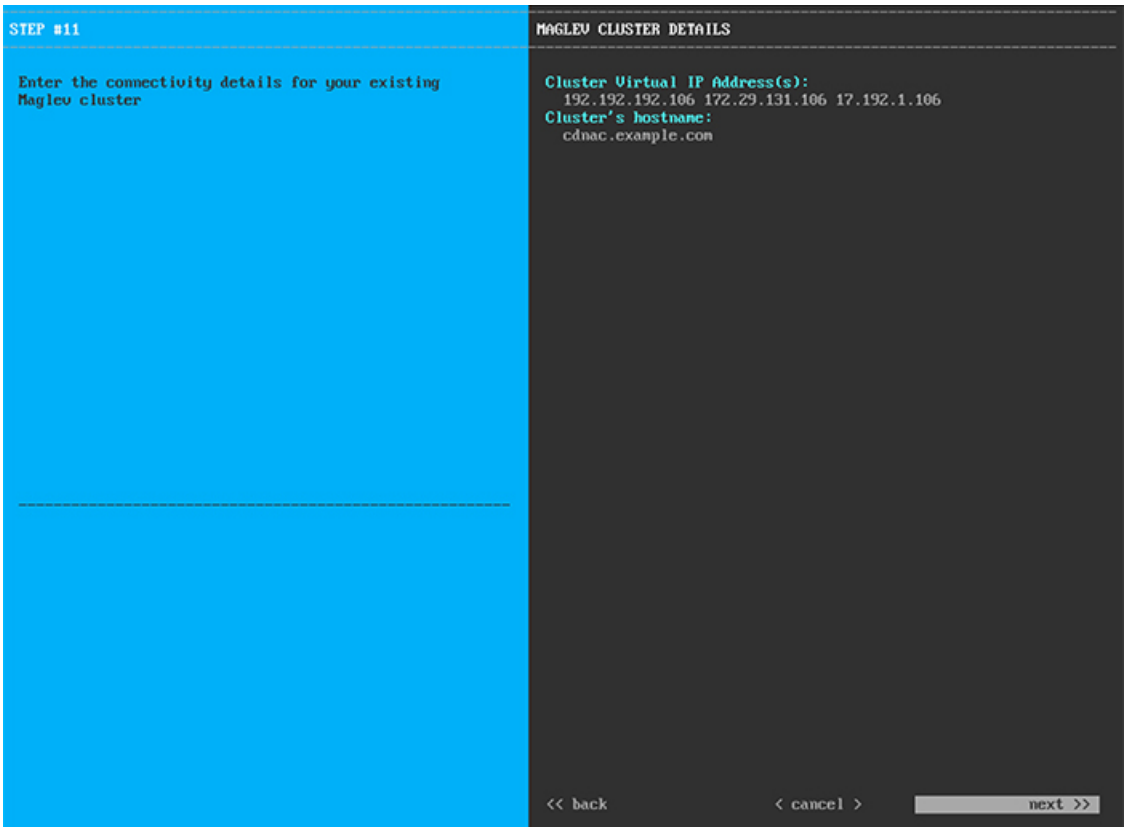

아래 표에 나와 있는 것처럼 **NETWORK PROXY**(네트워크 프록시)에 대한 구성 값을 입력합니다.

표 *26:* 네트워크 프록시에 대한 마스터 노드 항목

| | |
|---|---|
| **HTTPS** 프록시 | 인터넷에 액세스하는 데 사용되는 HTTPS 네트워크 프록시의 URL 또는 호스트 이름을 입력합니다.<br>참고 Cisco DNA Center에서 HTTPS 프록시로의 연결은 이 릴리스의 HTTP를 통해서만 지원됩니다. |
| **HTTPS Proxy Username(HTTPS** 프록시 사용자 이름**)** | 네트워크 프록시에 액세스하는 데 사용되는 사용자 이름을 입력합니다. 프록시 로그인이 필요하지 않은 경우 이 필드를 비워둡니다. |
| **HTTPS Proxy Password(HTTPS** 프록시 비밀번호**)** | 네트워크 프록시에 액세스하는 데 사용되는 비밀번호를 입력합니다. 프록시 로그인이 필요하지 않은 경우 이 필드를 비워둡니다. |

작업을 완료하면 **next>>(**다음**>>)**를 입력하여 계속 진행합니다. 이전 화면에서 수행한 것처럼 유효성 검사 오류를 수정합니다.

단계 **10** 네트워크 프록시 구성이 완료되면 마법사에서는 아래에 나와 있는 것처럼 **MAGLEV CLUSTER DETAILS(MAGLEV** 클러스터 세부 정보**)**에서 마스터 노드에 대한 가상 IP 주소를 입력하라는 프롬프트를 표시합니다.



클러스터와 네트워크 간의 트래픽에 사용되는 가상 IP 주소를 공백으로 구분한 목록을 입력합니다. 이는 향후 3개의 노드로 이루어진 클러스터로 변환될 단일 노드 클러스터 및 3개의 노드로 이루어진 클러스터에 모두 필요합니다. 단일 노드 클러스터 설정이 있고 이를 유지하려는 경우 이 단계를 건너뛰고 11단계로 이동합니다.

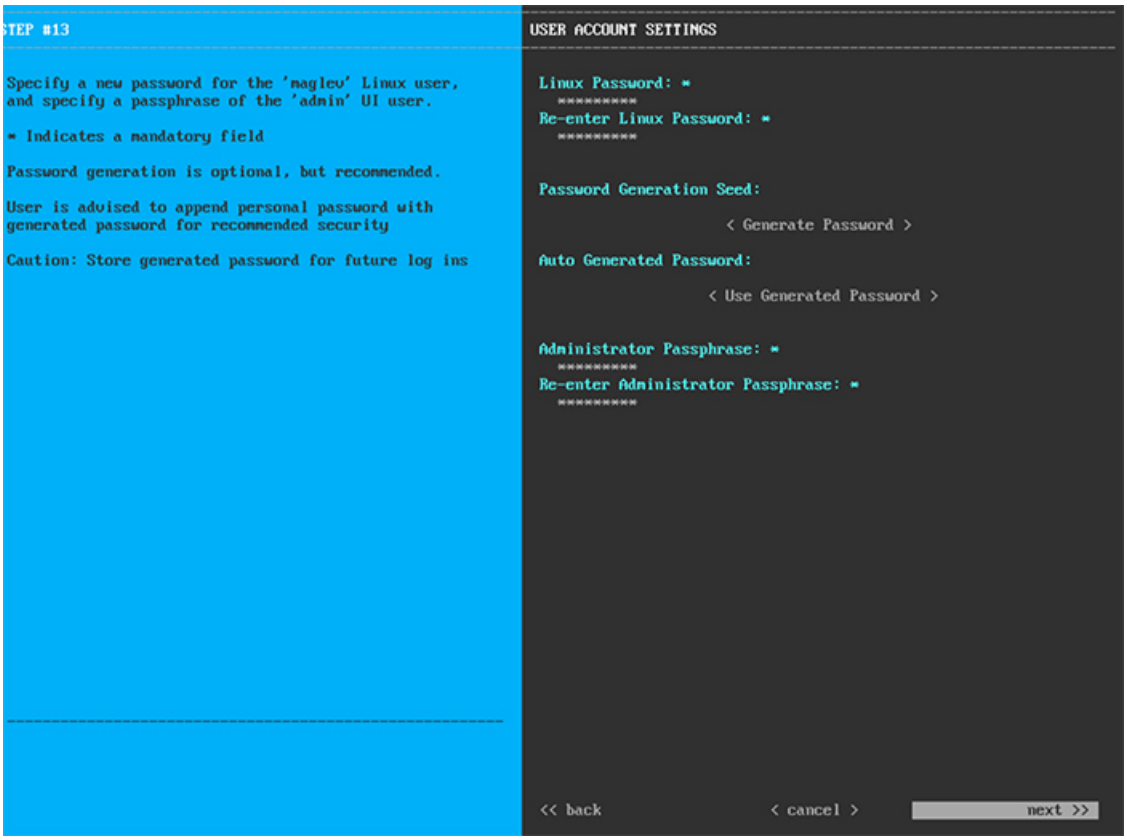
중요 구성된 각 네트워크 인터페이스에 하나의 가상 IP 주소를 입력해야 합니다. 이 작업을 수행하지 않으면 마법사를 완료할 수 없습니다. 이러한 주소는 클러스터 링크의 상태에 연결되며, 이는 **UP(**작동**)** 상태여야 합니다.

또한 클러스터에 대한 FQDN(Fully Qualified Domain Name)을 지정하는 옵션도 있습니다. Cisco DNA Center에서는 이 호스트 이름을 사용하여 다음 작업을 수행합니다.

- 이 호스트 이름을 사용하여 클러스터의 웹 인터페이스 및 Cisco DNA Center에서 관리하는 엔터프라이즈 네트워크의 디바이스에서 사용하는 REST(Representational State Transfer) API에 액세스합니다.
- Cisco DNA Center 인증서의 SAN(Subject Alternative Name) 필드에서 FQDN을 사용하여 디바이스 프로비저닝에 사용해야 하는 플러그 앤 플레이 서버를 정의합니다.

작업을 완료하면 **next>>(**다음>>**)**를 입력하여 계속 진행합니다. 이전 화면에서 수행한 것처럼 유효성 검사 오류를 수정합니다.

단계 **11** 가상 IP 주소가 입력되면 마법사에서는 아래에 나와 있는 것처럼 **USER ACCOUNT SETTINGS(**사용자 어카운트 설정**)**에 대한 값을 입력하라는 프롬프트를 표시합니다.



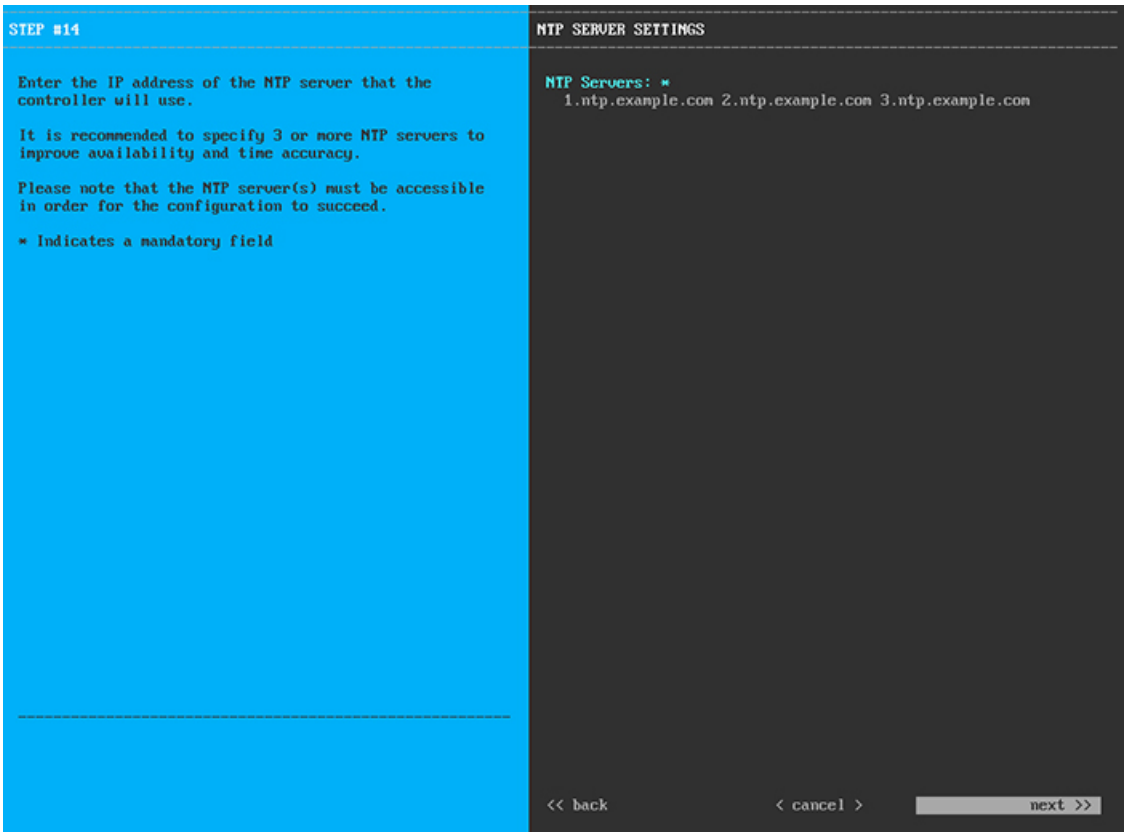

아래의 표에 나와 있는 것처럼 **USER ACCOUNT SETTINGS(**사용자 어카운트 설정**)**에 대한 값을 입력합니다.

표 *27:* 사용자 어카운트 설정에 대한 마스터 노드 항목

| | |
|---|---|
| **Linux Password(Linux** 비밀번호**)** | maglev 사용자용 Linux 비밀번호를 입력합니다. |
| **Re-enter Linux Password(Linux** 비밀번호 재입력**)** | Linux 비밀번호를 다시 입력하여 확인합니다. |
| **Password Generation Seed(**비밀번호 생성 시드**)** | Linux 비밀번호를 직접 생성하지 않으려면 이 필드에 시드 구문을 입력한 다음, <**Generate Password**>(비밀번호 생성)를 눌러 비밀번호를 생성합니다. |
| **Auto Generated Password(**자동 생성 비밀번호**)** | (선택 사항) 시드 프레이즈는 임의 보안 비밀번호의 일부로 나타납니다. 필요에 따라 자동 생성된 이 비밀번호를 "그대로" 사용하거나 수정할 수 있습니다.<br><**Use Generated Password(**생성된 비밀번호 사용**)**>를 눌러 비밀번호를 저장합니다. |
| 관리자 암호 | Cisco DNA Center에 처음 로그인할 때 사용하는 기본 관리 수퍼 사용자의 비밀번호를 입력합니다. |
| **Re-enter Administrator Passphrase(**관리자 암호 재입력**)** | 관리자 암호를 다시 입력하여 확인합니다. |

작업을 완료하면 **next>>(**다음**>>)**를 입력하여 계속 진행합니다. 이전 화면에서 수행한 것처럼 유효성 검사 오류를 수정합니다.

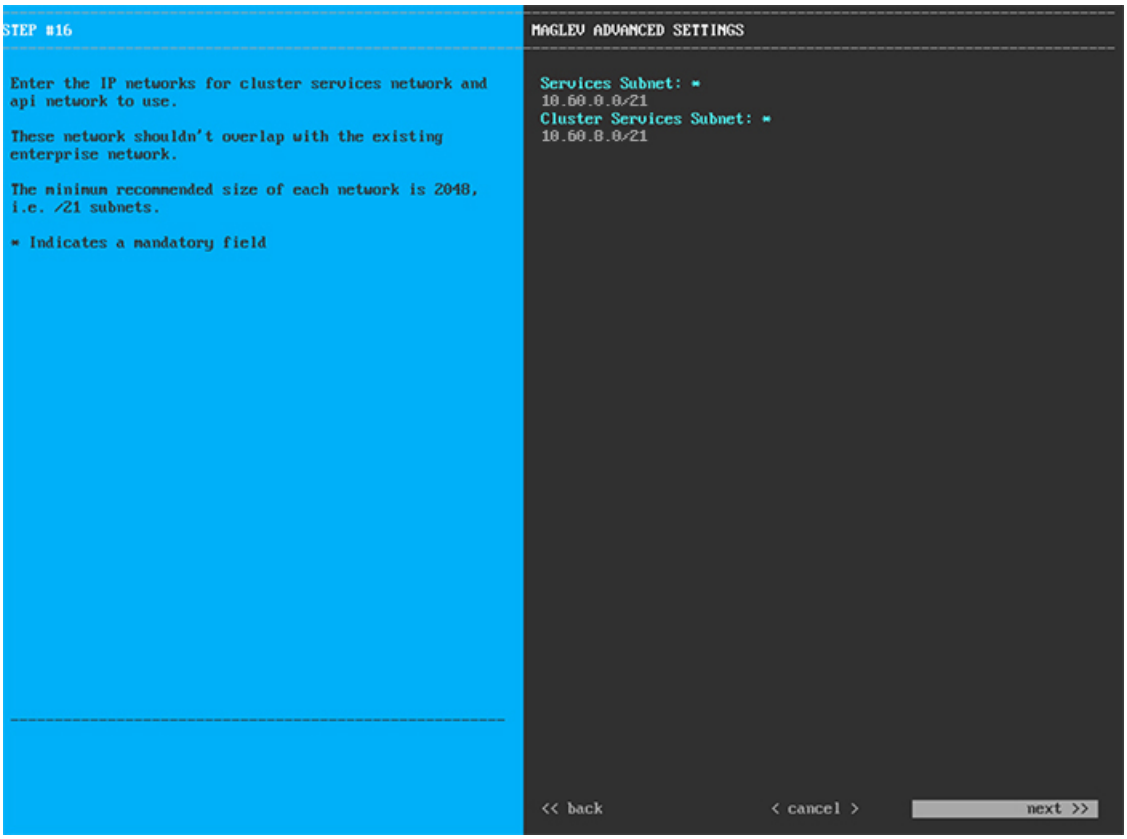
단계 **12** 사용자 어카운트 세부 정보가 입력되면 마법사에서는 아래에 나와 있는 것처럼 **NTP SERVER SETTINGS(NTP** 서버 설정**)**에 대한 값을 입력하라는 프롬프트를 표시합니다.




하나 이상의 NTP 서버 주소 또는 호스트 이름을 공백으로 구분하여 입력합니다. 하나 이상의 NTP 주소 또는 호스트 이름이 필요합니다. 프로덕션 구축의 경우 최소 3개의 NTP 서버를 구성하는 것이 좋습니다.

작업을 완료하면 **next>>(**다음**>>)**를 입력하여 계속 진행합니다. 이전 화면에서 수행한 것처럼 유효성 검사 오류를 수정합니다. 마법사에서 NTP 서버 구성을 검증하고 적용합니다.

단계 **13** NTP 서버를 지정하고 나면 마법사에서는 아래에 나와 있는 것처럼 **MAGLEV ADVANCED SETTINGS(MAGLEV** 고급 설정**)**에 대한 값을 입력하라는 프롬프트를 표시합니다.



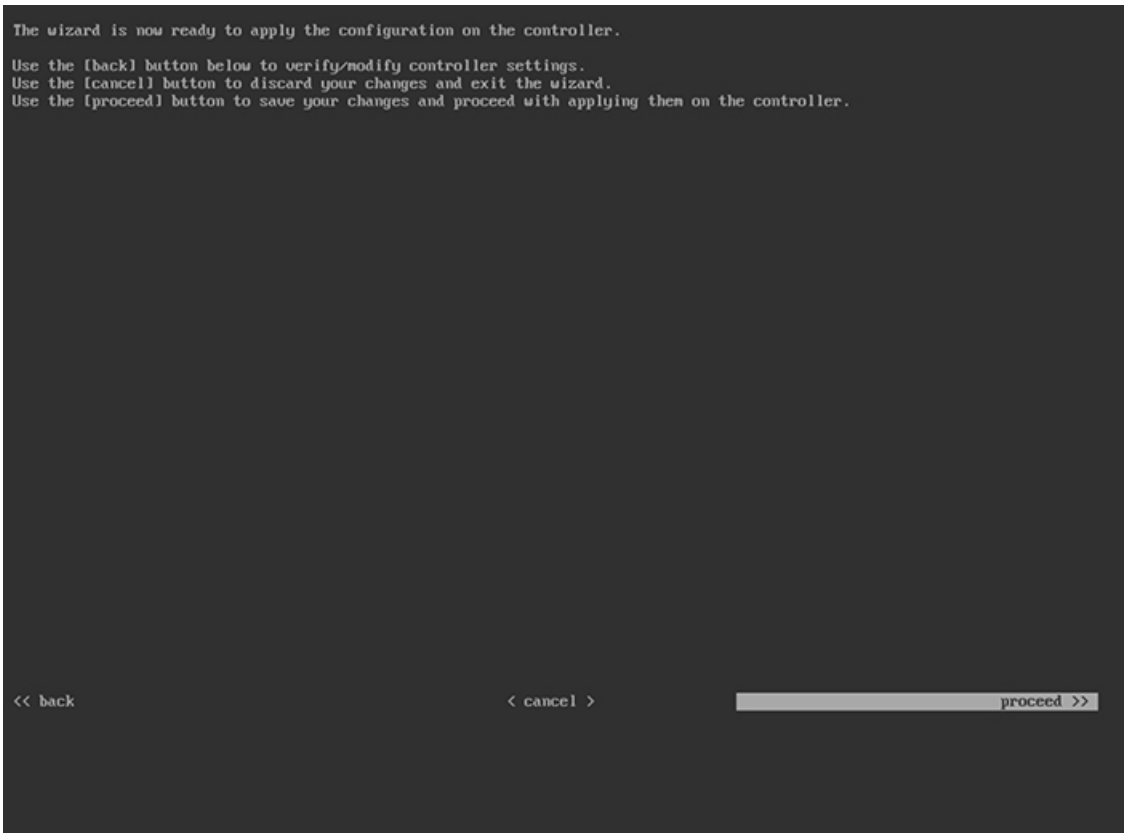

아래 표에 나와 있는 것처럼 **MAGLEV ADVANCED SETTINGS(MAGLEV** 고급 설정**)**에 대한 구성 값을 입력합니다.

표 ***28: Maglev*** 고급 설정에 대한 마스터 노드 항목

| | |
|---|---|
| **Services Subnet(**서비스 서브넷**)** | 자체 서비스를 관리하는 데 사용할 Cisco DNA Center의 전용 IP 서브넷을 입력합니다. |
| **Cluster Services Subnet(**클러스터 서비스 서브넷**)** | 클러스터링 서비스를 관리하는 데 사용할 Cisco DNA Center의 전용 IP 서브넷을 입력합니다. |

작업을 완료하면 **next>>(**다음**>>)**를 입력하여 계속 진행합니다. 이전 화면에서 수행한 것처럼 유효성 검사 오류를 수정합니다.

단계 **14** Maglev Advanced Settings(Maglev 고급 설정)의 입력을 마치면 마법사에서 구성을 적용할 준비가 되었음을 알리는 최종 메시지가 아래에 나와 있는 것처럼 나타납니다.




**proceed>>(**진행**>>)**를 입력하여 구성을 완료합니다.

설정이 적용되고 서비스가 표시되면 호스트가 자동으로 리부팅되고 KVM 콘솔에 메시지가 표시됩니다. 이 프로세스에는 몇 시간 정도 걸릴 수 있습니다. KVM 콘솔을 통해 진행 상황을 모니터링할 수 있습니다.

구성 프로세스가 끝나면 어플라이언스의 전원이 꺼졌다 켜진 다음, **CONFIGURATION SUCCEEDED!(**구성 성공**!)** 메시지가 표시됩니다.

---

다음에 수행할 작업

이 작업이 완료되면 다음 작업을 수행합니다.

- 독립형 모드에서만 이 어플라이언스를 구축하는 경우에는 초기 설정 워크플로를 수행하여 계속 진행합니다.
- 이 Cisco DNA Center 어플라이언스를 클러스터에서 마스터 노드로 구축하는 경우, 클러스터에서 두 번째 및 세 번째로 설치된 어플라이언스를 구성합니다(추가 기능 노드 구성).

# 추가 기능 노드 구성

이 절차의 단계를 수행하여 클러스터에서 두 번째 및 세 번째 어플라이언스를 구성합니다.

중요 클러스터의 각 어플라이언스에 대해 해당 인터페이스 중 하나에서만 DNS 서버를 구성합니다. 여러 인터페이스에서 DNS 서버를 구성하는 경우 문제가 발생할 수 있습니다.

각각의 새로운 추가 기능 노드를 클러스터에 조인할 때 클러스터의 첫 번째 호스트를 마스터 노드로 지정해야 합니다. 클러스터에 추가 기능 노드를 조인할 때는 다음 사항에 유의하십시오.

- 클러스터에는 한 번에 하나의 노드만 조인해야 합니다. 여러 노드를 동시에 추가하지 마십시오. 이렇게 하면 예기치 않은 동작이 발생할 수 있습니다.
- 클러스터에 새 노드를 추가하기 전에 설치된 모든 패키지가 마스터 노드에 구축되어 있는지 확인하십시오. 이는 Secure Shell을 사용해 마스터 노드의 Cisco DNA Center GUI 포트에 Linux 사용자(maglev)로 로그인한 다음, `maglev package status` 명령을 실행하여 확인할 수 있습니다. 설치된 모든 패키지는 명령 출력에 `DEPLOYED`(구축됨)로 표시되어야 합니다. 다음 예에서는 application-policy, sd-access, sensor-assurance, sensor-automation 패키지가 설치되지 않았으므로 이러한 패키지의 상태만 `NOT_DEPLOYED`(구축되지 않음)입니다. 추가 기능 노드를 구성하기 전에는 패키지 상태가 이와 유사하게 표시됩니다.

```
$ ssh maglev@172.29.131.14 -p 2222
The authenticity of host '[172.29.131.14]:2222 ([172.29.131.14]:2222)' can't be
established.
ECDSA key fingerprint is SHA256:scye+2ll6NFHAkOZDs0cNLHBR75j1KV3ZXIKuUaiadk.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '[172.29.131.14]:2222' (ECDSA) to the list of known hosts.
Welcome to the Maglev Appliance
maglev@172.29.131.14's password:

Welcome to the Maglev Appliance

System information as of Thu Dec 20 03:07:13 UTC 2018

System load: 4.08                   IP address for enp9s0: 17.192.1.14
Usage of /: 59.8% of 28.03GB        IP address for enp10s0: 192.192.192.14
Memory usage: 21%                   IP address for enp1s0f0: 172.29.131.14
Swap usage: 0%                      IP address for docker0: 169.254.0.1
Processes: 831                      IP address for tun10: 10.60.3.0
Users logged in: 0

To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

[Thu Dec 20 03:07:13 UTC] maglev@192.192.192.14 (maglev-master-1) ~
$ maglev package status
[administration] password for 'admin':

maglev-1 [main - https://kong-frontend.maglev-system.svc.cluster.local:443]

NAME                            DEPLOYED        AVAILABLE       STATUS
-------------------------------------------------------------------------------------
application-policy              -               2.1.10.170000   NOT_DEPLOYED
assurance                       1.0.5.686       1.1.8.1440      DEPLOYED
automation-core                 2.1.8.60044     2.1.12.60011    DEPLOYED
base-provision-core             2.1.8.60044     2.1.12.60016    DEPLOYED
command-runner                  2.1.8.60044     2.1.9.60029     DEPLOYED
device-onboarding               2.1.8.60044     2.1.12.60016    DEPLOYED
image-management                2.1.8.60044     2.1.12.60011    DEPLOYED
ncp-system                      2.1.8.60044     2.1.9.60029     DEPLOYED
ndp-base-analytics              1.0.7.878       1.0.7.908       DEPLOYED
```

```
ndp-platform                1.0.7.829       1.0.7.866       DEPLOYED
ndp-ui                      1.0.7.956       1.0.7.975       DEPLOYED
network-visibility          2.1.8.60044     2.1.12.60016    DEPLOYED
path-trace                  2.1.8.60044     2.1.12.60016    DEPLOYED
sd-access                   -               2.1.12.60016    NOT_DEPLOYED
sensor-assurance            -               1.1.5.40        NOT_DEPLOYED
sensor-automation           -               2.1.9.60029     NOT_DEPLOYED
system                      1.0.4.807       1.0.4.855       DEPLOYED
```

- 각 추가 기능 노드에 대한 클러스터 첨부 프로세스가 진행되는 동안에는 어느 정도 서비스 다운타임이 예상됩니다. 서비스는 노드 전체에 재배포되어야 하며 해당 프로세스가 진행되는 동안에는 클러스터의 작동이 중단됩니다.

시작하기 전에

확인:

- 마스터 노드 구성 단계를 수행하여 클러스터에서 첫 번째 어플라이언스를 구성했는지 확인합니다.
- 필수 서브넷 및 추가 IP 주소 및 필수 구성 정보에서 요구하는 모든 정보를 수집했습니다.
- 어플라이언스 설치 워크플로에 설명된 대로 두 번째 및 세 번째 어플라이언스를 설치했는지 확인합니다.
- CIMC에 대한 브라우저 액세스 활성화에 설명된 대로 두 개의 추가 기능 어플라이언스에서 모두 CIMC 브라우저 액세스를 구성했는지 확인합니다.
- 사전 검사 실행에 설명된 대로 추가 기능 노드 어플라이언스의 포트와 그에 의해 사용되는 스위치가 올바르게 구성되었는지 확인합니다.
- CIMC 및 Cisco DNA Center와 호환 가능한 브라우저를 사용하고 있습니다. 호환되는 브라우저 목록은 설치 중인 Cisco DNA Center 버전에 대한 릴리스 노트를 참조하십시오.
- 다음 절차의 8단계에서 지정하는 Cisco DNA Center와 DNS 서버 간의 방화벽에서 ICMP를 활성화했습니다. Maglev 구성 마법사는 Ping을 사용하여 사용자가 지정하는 DNS 서버를 확인합니다. Cisco DNA Center와 DNS 서버 간에 방화벽이 있고 해당 방화벽에서 ICMP가 활성화되지 않은 경우 이 ping을 차단할 수 있습니다. 이 경우에는 마법사를 완료할 수 없습니다.

---

단계 **1** 사용자가 수행한 CIMC GUI 구성 중에 설정한 CIMC IP 주소를 브라우저에서 확인하고 CIMC GUI에 CIMC 사용자로 로그인합니다(CIMC에 대한 브라우저 액세스 활성화 참조).

로그인이 완료되면 다음 그림과 같이 어플라이언스에 **Cisco Integrated Management Controller** 섀시 요약 창이 표시되고 오른쪽 상단에 파란색 링크 메뉴가 표시됩니다.

단계 **2** 파란색 링크 메뉴에서 **Launch KVM(KVM** 실행**)**을 선택한 다음 **Java based KVM(Java** 기반 **KVM)** 또는 **HTML based KVM(HTML** 기반 **KVM)** 중 하나를 선택합니다. Java 기반 KVM을 선택하는 경우에는 브라우저 또는 파일 관리자에서 Java 시작 파일을 실행 하여 KVM 콘솔을 콘솔 창에서 확인해야 합니다. HMTL 기반 KVM을 선택하는 경우에는 KVM 콘솔이 별도의 브라우저 창 또는 탭에서 자동으로 실행됩니다.

선택한 KVM 유형과 관계 없이 KVM 콘솔을 사용하여 구성의 진행 상황을 모니터링하고 Maglev 구성 마법사 프롬프트에 응답합니다.

단계 **3** KVM이 표시되 면 다음 선택 사항 중 하나를 수행하여 어플라이언스를 리부팅합니다.

a) 기본 CIMC GUI 브라우저 창에서 **Host Power(**호스트 전원**)** > **Power Cycle(**전원 껐다 켜기**)**을 선택합니다. 그런 다음 KVM 콘솔로 전환하여 작업을 계속합니다.

b) KVM 콘솔에서 **Power(**전원**)** > **Power Cycle System (cold boot)(**시스템 껐다 켜기**(**콜드 부트**))**을 선택합니다.

어플라이언스를 리부팅할 것인지 선택하라는 프롬프트가 표시되면 **OK(**확인**)**를 클릭합니다.

리부팅 메시지를 표시한 후 KVM 콘솔에는 아래에 표시된 Maglev 구성 마법사 시작 화면이 표시됩니다.

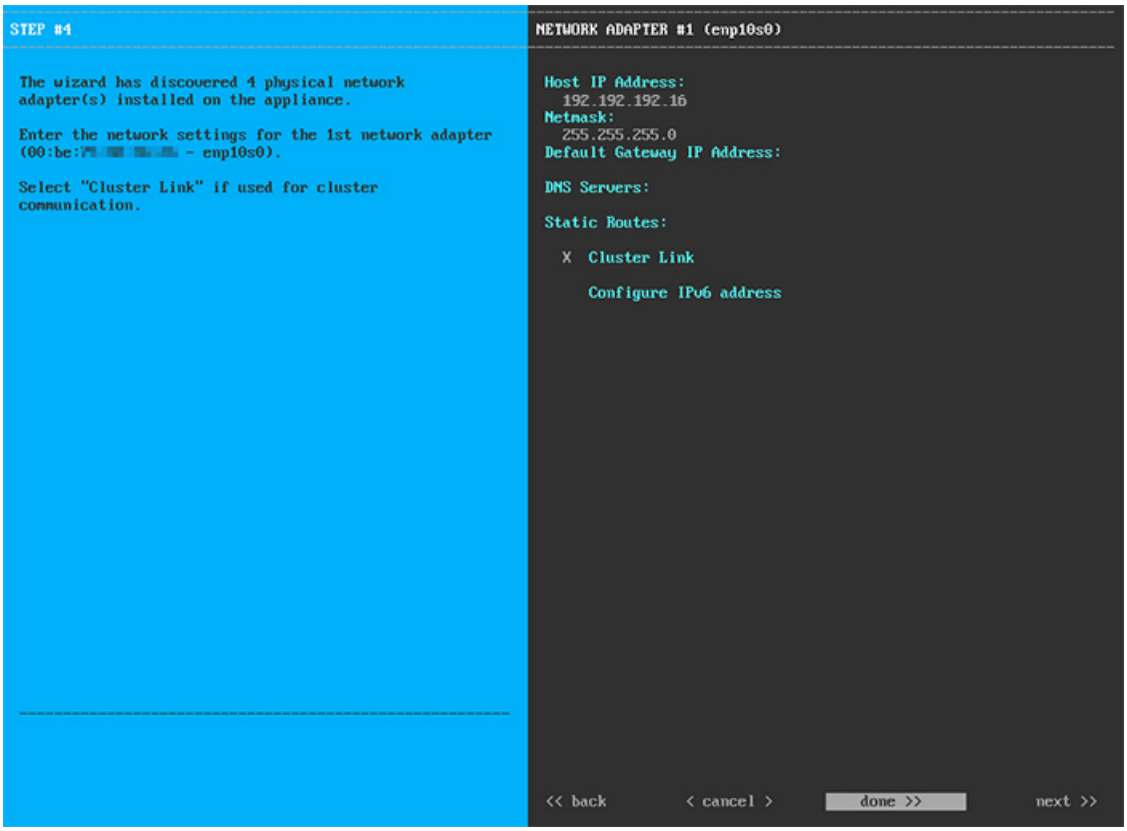
단계 **4** 추가 기능 노드 구성을 시작하려면 **Join a DNA-C cluster(DNA-C** 클러스터 조인**)**를 선택합니다.

마법사는 어플라이언스의 모든 포트를 검색하여 다음 순서대로 별도의 화면에 하나씩 표시합니다.

1. 10Gbps 클러스터 포트(포트 2, enp10s0, 네트워크 어댑터 #1)
2. 1Gbps Cisco DNA Center GUI 포트(1, enp1s0f0, 네트워크 어댑터 #2)
3. 1Gbps 클라우드 포트(2, enp1s0f1, 네트워크 어댑터 #3)
4. 10Gbps 엔터프라이즈 포트(포트 1, enp9s0, 네트워크 어댑터 #4)

참고 구성 과정에서 마법사가 10Gbps 포트 중 하나 또는 둘 다를 표시하지 못하면 이러한 포트가 작동하지 않거나 비활성화될 수 있습니다. 이러한 10Gbps 포트는 Cisco DNA Center 기능에 필요합니다. 이러한 포트가 작동하지 않는 것을 발견하면 **cancel(**취소**)**을 선택하여 즉시 구성을 종료합니다. 구성을 다시 시작하거나 Cisco TAC(Technical Assistance Center)에 연결하기 전에 사전 검사 실행에서 제공된 모든 단계를 완료했는지 확인하십시오.

단계 **5** 마법사는 10Gbps 클러스터 포트(포트 2, enp10s0)를 먼저 검색하여 네트워크 어댑터 **#1**을 표시합니다. 인터페이스 케이블 연결에 설명된 것처럼 이 포트는 어플라이언스를 클러스터에 연결하는 데 사용되므로 이 목적에 적합한 호스트 IP 주소, 넷마스크 및 기타 값을 적용합니다(입력할 값은 필수 서브넷 및 추가 IP 주소, 필수 구성 정보 참조).




아래 표에 나와 있는 것처럼 네트워크 어댑터 **#1**에 대한 구성 값을 입력합니다.

표 ***29:*** 네트워크 어댑터 ***#1: 10Gbps*** 클러스터 포트***(enp10s0)***에 대한 추가 기능 노드 항목

| | |
|---|---|
| **Host IP address**(호스트 **IP** 주소) | 클러스터 포트의 IP 주소를 입력합니다. 이는 필수 항목입니다. 나중에 클러스터 포트의 주소를 변경할 수 없습니다. |
| **Netmask** | 포트의 IP 주소에 대한 넷마스크를 입력합니다. 이는 필수 값입니다. |
| **Default Gateway IP address**(기본 게이트웨이 **IP** 주소) | 포트에 사용할 기본 게이트웨이 IP 주소를 입력합니다. 이는 일반적으로 엔터프라이즈 포트에만 필요합니다. |
| **DNS** 서버 | 기본 설정된 DNS 서버의 IP 주소를 입력합니다. 여러 DNS 서버를 입력하는 경우 목록에 있는 IP 주소를 공백으로 구분합니다. |
| **Static Routes**(고정 경로) | 다음 형식으로 하나 이상의 정적 경로를 공백으로 구분하여 입력합니다. <network>/<netmask>/<gateway>. 이는 일반적으로 Cisco DNA Center GUI 포트에만 필요합니다. |

| | |
|---|---|
| 클러스터 링크 | 이 포트를 클러스터에 대한 링크로 지정하려면 확인란을 선택합니다. 이는 클러스터 포트에만 필요합니다. |
| **IPv6** 주소 구성 | 이후 사용을 위해 예약됩니다. 이 필드는 비워둡니다. |

구성 값을 입력했으면 **next>>(**다음**>>)**를 입력하여 계속 진행합니다. **next>>(**다음**>>)**를 입력한 후에 마법사에서 입력한 값의 유효성 검사를 수행하고 잘못된 경우 오류 메시지를 표시합니다. 오류 메시지를 수신하면 입력한 값이 정확한지 확인한 다음 다시 입력합니다. 필요한 경우 **<< back(**뒤로**)**을 선택하여 다시 입력합니다.

단계 **6** 입력한 클러스터 포트 값의 검증이 완료되면 마법사는 1Gbps Cisco DNA Center GUI 포트(1, enp1s0f0)를 네트워크 어댑터 **#2**로 제공합니다. 인터페이스 케이블 연결에서 설명하는 것처럼 이 포트는 관리 네트워크에서 Cisco DNA Center GUI에 액세스하는 데 사용됩니다. 이 목적에 적합한 호스트 IP 주소, 넷마스크 및 기타 값을 적용합니다(필수 서브넷 및 추가 IP 주소 및 필수 구성 정보 참조).

아래 표에 나와 있는 것처럼 네트워크 어댑터 **#2**에 대한 구성 값을 입력합니다.

표 ***30:*** 네트워크 어댑터 ***#2: 1Gbps GUI*** 포트***(enp1s0f0)***에 대한 추가 기능 노드 항목

| | |
|---|---|
| **Host IP address(**호스트 **IP** 주소**)** | 1Gpbs Cisco DNA Center GUI 포트의 IP 주소를 입력합니다. 이는 필수 값입니다. |
| **Netmask** | 포트의 IP 주소에 대한 넷마스크를 입력합니다. 이는 필수 값입니다. |

| | |
|---|---|
| **Default Gateway IP address(**기본 게이트웨이 **IP** 주소**)** | 포트에 사용할 기본 게이트웨이 IP 주소를 입력합니다. 이는 일반적으로 엔터프라이즈 포트에만 필요합니다. |
| **DNS** 서버 | 기본 설정된 DNS 서버의 IP 주소를 입력합니다. 여러 DNS 서버를 입력하는 경우 목록에 있는 IP 주소를 공백으로 구분합니다.<br>참고 NTP의 경우에는 Cisco DNA Center 및 NTP 서버 간에 포트 121(UDP)이 열려 있는지 확인합니다. |
| **Static Routes(**고정 경로**)** | 다음 형식으로 하나 이상의 정적 경로를 공백으로 구분하여 입력합니다. <network>/<netmask>/<gateway>. |
| 클러스터 링크 | 이 필드는 비워둡니다. 이는 클러스터 포트에만 필요합니다. |
| **IPv6** 주소 구성 | 이후 사용을 위해 예약됩니다. 이 필드는 비워둡니다. |

작업을 완료하면 **next>>(**다음**>>)**를 입력하여 계속 진행합니다. 이전 화면에서 수행한 것처럼 유효성 검사 오류를 수정합니다.

단계 **7** 입력한 Cisco DNA Center GUI 포트 값의 검증이 완료되면 마법사는 1Gbps 클라우드 포트(2, enp1s0f1)를 네트워크 어댑터 **#3**으로 제공합니다. 인터페이스 케이블 연결에 설명된 것처럼 10Gbps 엔터프라이즈 포트(포트 1, enp9s0)를 통해 어플라이언스를 인터넷에 연결하는 데 사용되는 선택 사항인 포트입니다. 이 목적에 적합한 호스트 IP 주소, 넷마스크 및 기타 값을 적용합니다(필수 서브넷 및 추가 IP 주소 및 필수 구성 정보 참조).

아래 표에 나와 있는 것처럼 네트워크 어댑터 **#3**에 대한 구성 값을 입력합니다.

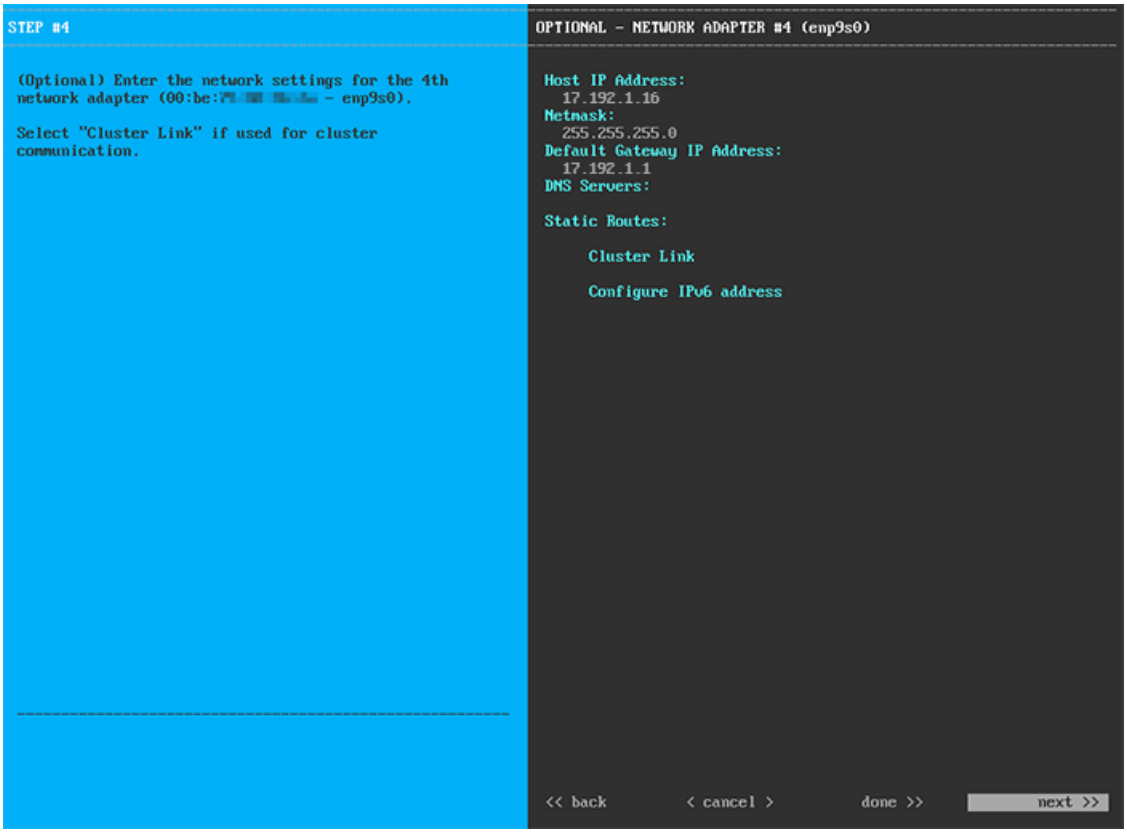
표 ***31:*** 네트워크 어댑터 ***#3: 1Gbps*** 클라우드 포트***(enp1s0f1)***에 대한 추가 기능 노드 항목

| | |
|---|---|
| **Host IP address**(호스트 **IP** 주소) | 클라우드 포트의 IP 주소를 입력합니다. 이는 인터넷 연결에 클라우드 포트를 사용하는 경우에만 필요합니다. 그렇지 않은 경우에는 비워둘 수 있습니다. |
| **Netmask** | 포트의 IP 주소에 대한 넷마스크를 입력합니다. 이는 IP 주소를 입력하는 경우 필요합니다. |
| **Default Gateway IP address**(기본 게이트웨이 **IP** 주소) | 클라우드 포트에 사용할 기본 게이트웨이 IP 주소를 입력합니다. 이는 일반적으로 엔터프라이즈 포트에만 필요합니다. |
| **DNS** 서버 | 기본 설정된 DNS 서버의 IP 주소를 입력합니다. 여러 DNS 서버를 입력하는 경우 목록에 있는 IP 주소를 공백으로 구분합니다. |
| **Static Routes**(고정 경로) | 다음 형식으로 하나 이상의 정적 경로를 공백으로 구분하여 입력합니다. <network>/<netmask>/<gateway>. 이는 일반적으로 GUI 포트에만 필요합니다. |

| | |
|---|---|
| 클러스터 링크 | 이 필드는 비워둡니다. 이는 클러스터 포트에만 필요합니다. |
| **IPv6** 주소 구성 | 이후 사용을 위해 예약됩니다. 이 필드는 비워둡니다. |

작업을 완료하면 **next>>(**다음>>**)**를 입력하여 계속 진행합니다. 이전 화면에서 수행한 것처럼 유효성 검사 오류를 수정합니다.

단계 **8** 입력한 클라우드 포트 값의 검증이 완료되면 마법사는 10Gbps 엔터프라이즈 포트( 포트 1, enp9s0)를 네트워크 어댑터 **#4**로 제공합니다. 인터페이스 케이블 연결에서 설명하는 것처럼, 이 포트는 어플라이언스를 엔터프라이즈 네트워크에 연결하는 데 사용되는 필수 포트입니다. 이 목적에 적합한 호스트 IP 주소, 넷마스크 및 기타 값을 적용합니다(필수 서브넷 및 추가 IP 주소 및 필수 구성 정보 참조).




아래 표에 나와 있는 것처럼 네트워크 어댑터 **#4**에 대한 구성 값을 입력합니다.

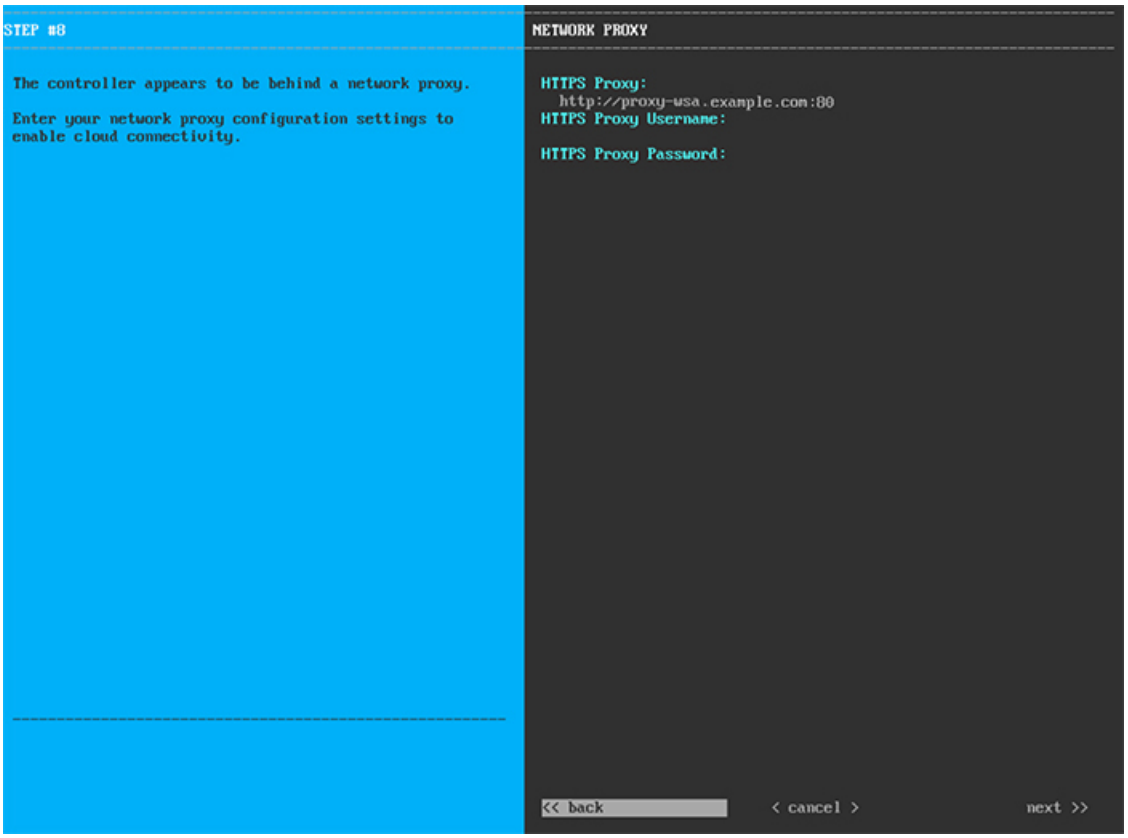
표 ***32:*** 네트워크 어댑터 ***#4: 10Gbps*** 엔터프라이즈 포트***(enp9s0)***에 대한 추가 기능 노드 항목

| | |
|---|---|
| **Host IP address(**호스트 **IP** 주소**)** | 10Gpbs 엔터프라이즈 포트의 IP 주소를 입력합니다. 이는 필수 값입니다. |
| **Netmask** | 포트의 IP 주소에 대한 넷마스크를 입력합니다. 이는 필수 값입니다. |

| | |
|---|---|
| **Default Gateway IP address(**기본 게이트웨이 **IP** 주소**)** | 포트에 사용할 기본 게이트웨이 IP 주소를 입력합니다. 이는 필수 값입니다. |
| **DNS** 서버 | 기본 설정된 DNS 서버의 IP 주소를 입력합니다. 여러 DNS 서버를 입력하는 경우 목록에 있는 IP 주소를 공백으로 구분합니다. |
| **Static Routes(**고정 경로**)** | 다음 형식으로 하나 이상의 정적 경로를 공백으로 구분하여 입력합니다. <network>/<netmask>/<gateway>. 이는 일반적으로 GUI 포트에만 필요합니다. |
| 클러스터 링크 | 이 필드는 비워둡니다. 이는 클러스터 포트에만 필요합니다. |
| **IPv6** 주소 구성 | 이후 사용을 위해 예약됩니다. 이 필드는 비워둡니다. |

작업을 완료하면 **next>>(**다음**>>)**를 입력하여 계속 진행합니다. 이전 화면에서 수행한 것처럼 유효성 검사 오류를 수정합니다.

단계 **9** 네트워크 어댑터 구성이 완료되면 마법사는 아래에 나와 있는 것처럼 사용 중인 네트워크 프록시에 대한 구성 값을 입력하라는 프롬프트를 표시합니다.



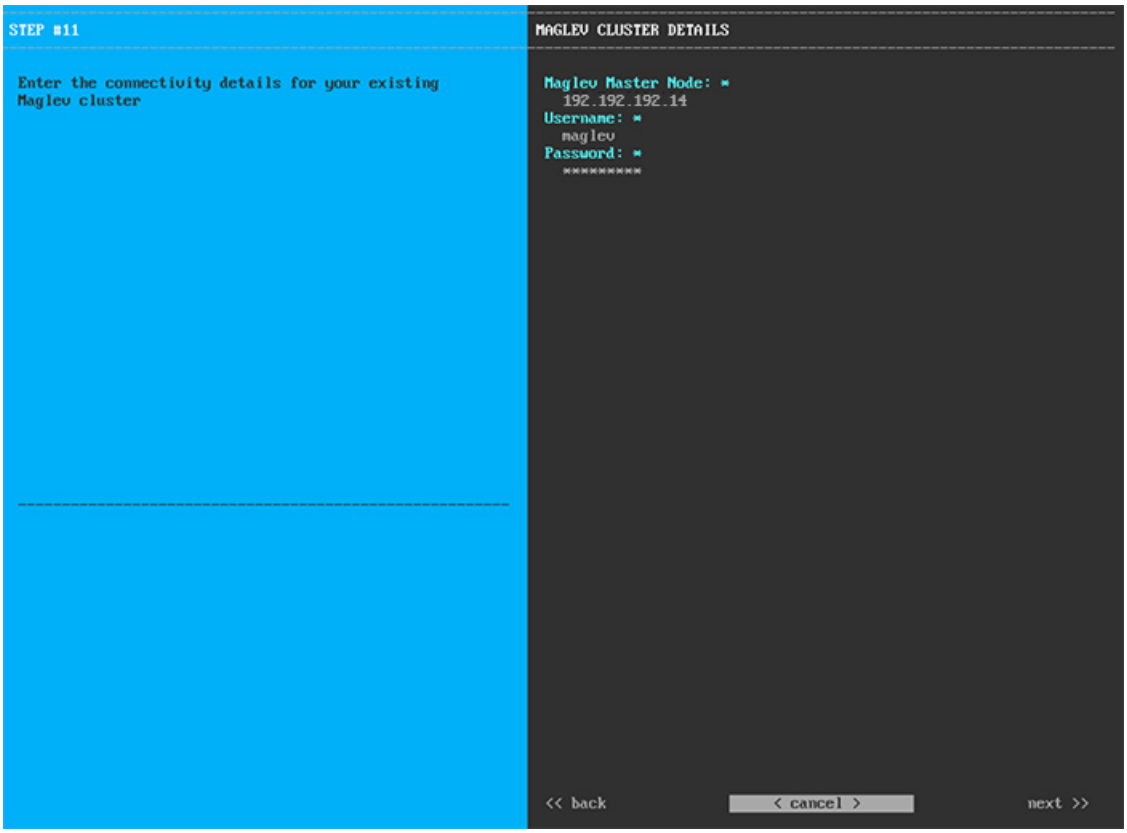

아래 표에 나와 있는 것처럼 네트워크 프록시에 대한 구성 값을 입력합니다.

표 ***33:*** 네트워크 프록시에 대한 추가 기능 노드 항목

| | |
|---|---|
| **HTTPS** 프록시 | 인터넷에 액세스하기 위한 HTTPS 네트워크 프록시의 URL 또는 호스트 이름을 입력합니다.<br>참고 Cisco DNA Center에서 HTTPS 프록시로의 연결은 이 릴리스의 HTTP를 통해서만 지원됩니다. |
| **HTTPS Proxy Username(HTTPS** 프록시 사용자 이름**)** | 네트워크 프록시에 액세스하는 데 사용되는 사용자 이름을 입력합니다. 프록시 로그인이 필요하지 않은 경우 이 필드를 비워둡니다. |
| **HTTPS Proxy Password(HTTPS** 프록시 비밀번호**)** | 네트워크 프록시에 액세스하는 데 사용되는 비밀번호를 입력합니다. 프록시 로그인이 필요하지 않은 경우 이 필드를 비워둡니다. |

작업을 완료하면 **next>>(**다음**>>)**를 입력하여 계속 진행합니다. 이전 화면에서 수행한 것처럼 유효성 검사 오류를 수정합니다.

단계 **10** 네트워크 프록시 구성이 완료되면 마법사에서는 아래에 나와 있는 것처럼 **MAGLEV CLUSTER DETAILS(MAGLEV** 클러스터 세부 정보**)**에서 마스터 노드의 클러스터 포트 및 마스터 노드 로그인 세부 정보를 식별하라는 프롬프트를 표시합니다.



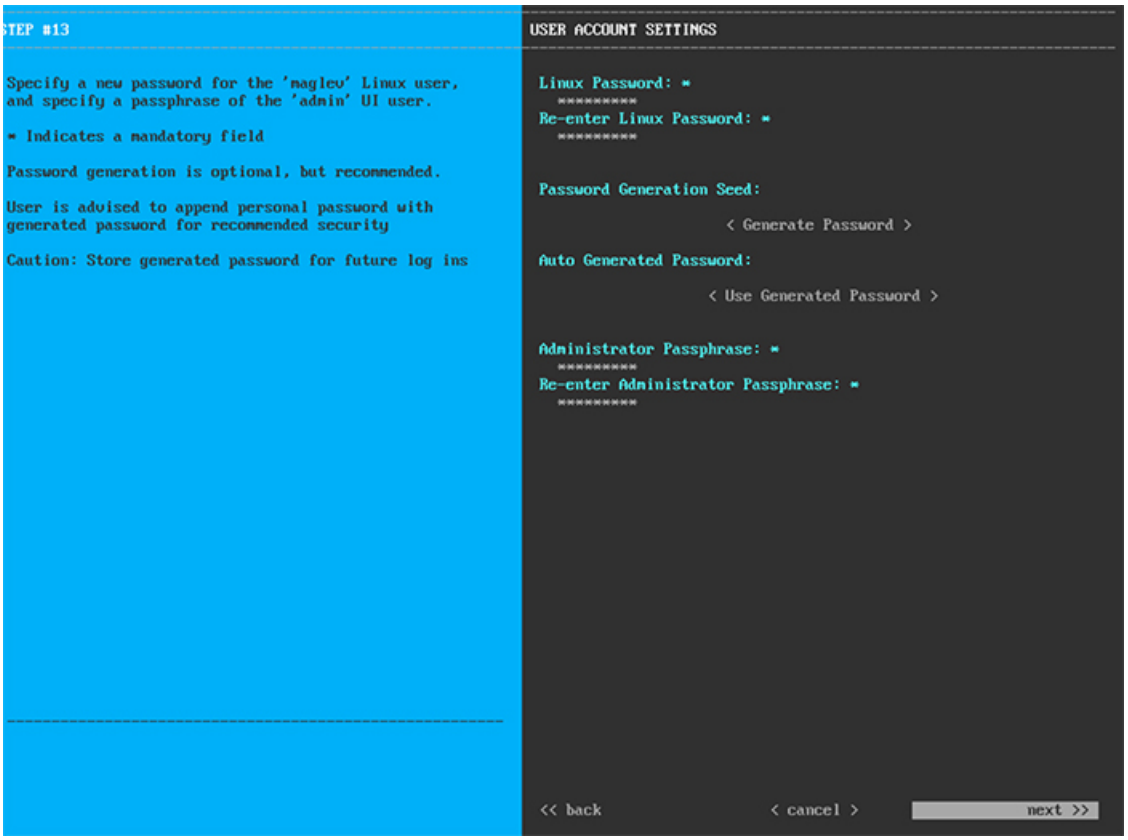
아래의 표에 나와 있는 것처럼 **MAGLEV CLUSTER DETAILS(MAGLEV** 클러스터 세부 정보)에 대한 값을 입력합니다.

표 ***34: Maglev*** 클러스터 세부 정보에 대한 추가 기능 노드 항목

| | |
|---|---|
| **Maglev Master Node(Maglev** 마스터 노드) | 클러스터 내 마스터 노드에 있는 클러스터 포트의 IP 주소를 입력합니다. 포트 할당에 대한 권장 사항을 준수한 경우, 이는 마스터 노드에서 포트 2, enp10s0, 네트워크 어댑터 #1의 IP 주소가 됩니다. |
| **User name(**사용자 이름) | **`maglev`**를 입력합니다. |
| 비밀번호 | 마스터 노드에서 구성한 Linux 비밀번호를 입력합니다. |

작업을 완료하면 **next>>(**다음**>>)**를 입력하여 계속 진행합니다. 이전 화면에서 수행한 것처럼 유효성 검사 오류를 수정합니다.

단계 **11** Maglev 클러스터 세부 정보가 입력되면 마법사에서는 아래에 나와 있는 것처럼 이 추가 기능 노드의 **USER ACCOUNT SETTINGS(**사용자 어카운트 설정)에 대한 값을 입력하라는 프롬프트를 표시합니다.



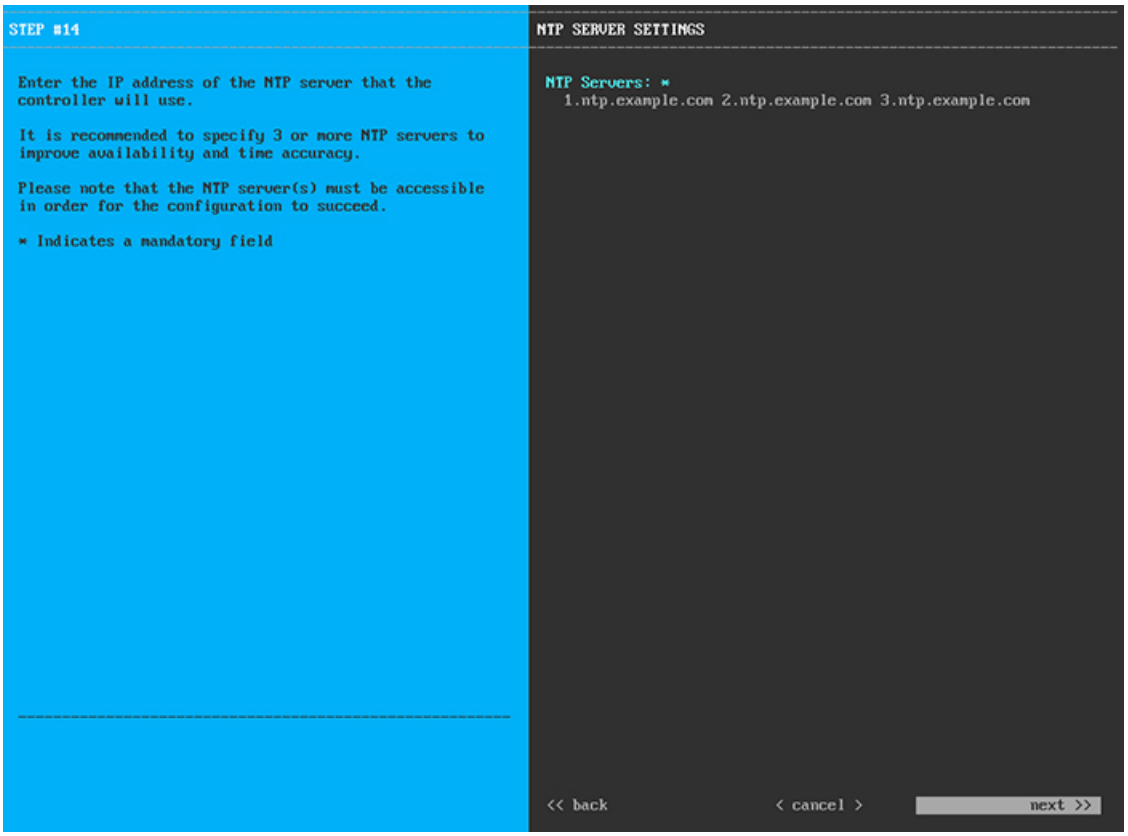

아래의 표에 표시된 것처럼 **USER ACCOUNT SETTINGS(**사용자 어카운트 설정)에 대한 값을 입력합니다.

표 ***35:*** 사용자 어카운트 설정에 대한 추가 기능 노드 항목

| | |
|---|---|
| **Linux Password(Linux** 비밀번호**)** | maglev 사용자용 Linux 비밀번호를 입력합니다. |
| **Re-enter Linux Password(Linux** 비밀번호 재입력**)** | Linux 비밀번호를 다시 입력하여 확인합니다. |
| 비밀번호 생성 시드 | Linux 비밀번호를 직접 생성하지 않으려면 이 필드에 시드 구문을 입력한 다음 <**Generate Password(**비밀번호 생성**)**>를 눌러 비밀번호를 생성합니다. |
| **Auto Generated Password(**자동 생성 비밀번호**)** | (선택 사항) 시드 프레이즈는 임의 보안 비밀번호의 일부로 나타납니다. 필요하다면 이 비밀번호를 "그대로" 사용하거나 이 자동 생성된 비밀번호를 추가로 수정할 수 있습니다.<br><**Use Generated Password(**생성된 비밀번호 사용**)**>를 눌러 비밀번호를 저장합니다. |
| 관리자 암호 | Cisco DNA Center에 처음 로그인할 때 사용하는 기본 관리자의 수퍼 사용자용 비밀번호를 입력합니다. |
| 관리자 암호 재입력 | 관리자 암호를 다시 입력하여 확인합니다. |

작업을 완료하면 **next>>(**다음>>**)**를 입력하여 계속 진행합니다. 이전 화면에서 수행한 것처럼 유효성 검사 오류를 수정합니다.

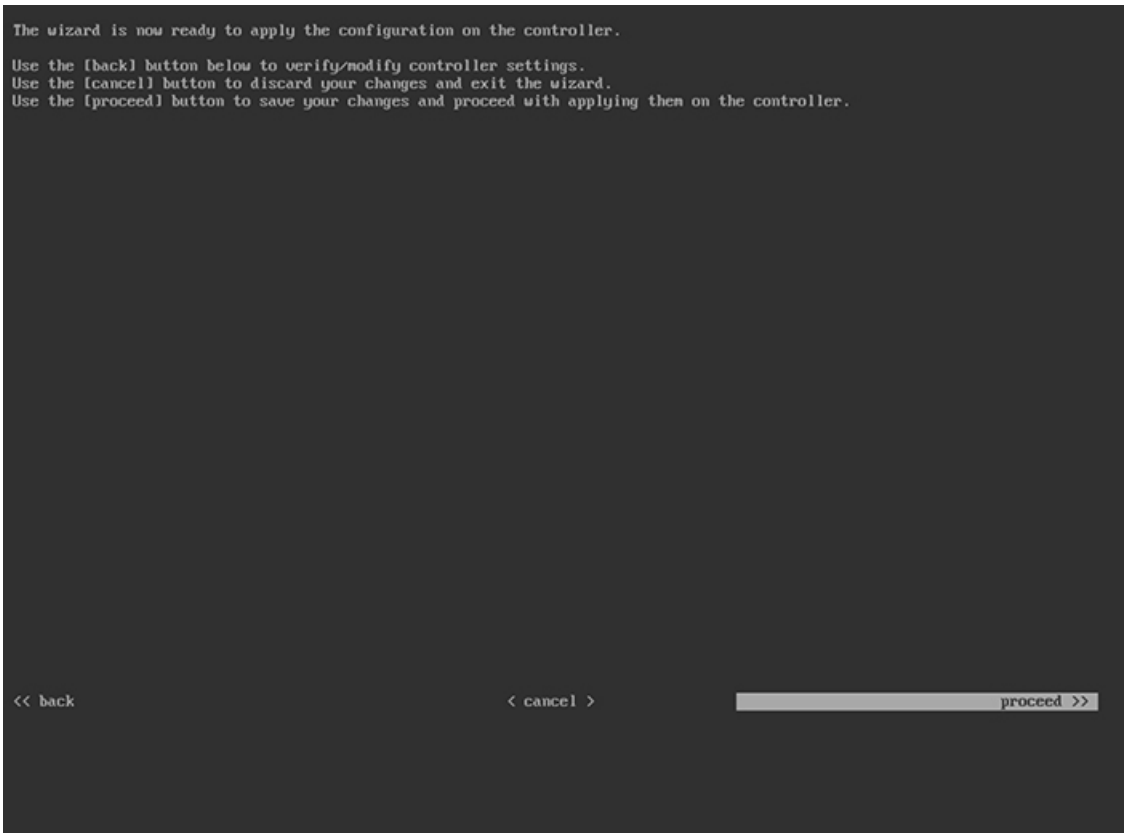
단계 **12** 사용자 어카운트 세부 정보가 입력되면 마법사는 아래에 표시된 대로 **NTP SERVER SETTINGS(NTP** 서버 설정**)**에 대한 값을 입력하라는 프롬프트를 표시합니다.




하나 이상의 NTP 서버 주소 또는 호스트 이름을 공백으로 구분하여 입력합니다. 하나 이상의 NTP 주소 또는 호스트 이름이 필요합니다. 이는 마스터 노드에 대해 지정한 것과 동일한 NTP 서버여야 합니다.

작업을 완료하면 **next>>(**다음**>>)**를 입력하여 계속 진행합니다. 이전 화면에서 수행한 것처럼 유효성 검사 오류를 수정합니다.

단계 **13** NTP Server Settings(NTP 서버 설정)의 입력을 마치면 마법사에서 구성을 적용할 준비가 되었음을 알리는 최종 메시지가 아래에 나와 있는 것처럼 나타납니다.




**proceed>>(**진행**)**를 입력하여 구성을 완료합니다.

호스트가 설정을 적용하고 서비스를 시작하면 호스트가 자동으로 리부팅되고 KVM 콘솔에 메시지가 표시됩니다. 이 프로세스에는 몇 시간 정도 걸릴 수 있습니다. KVM 콘솔을 통해 진행 상황을 모니터링할 수 있습니다.

구성 프로세스가 끝나면 어플라이언스의 전원이 꺼졌다 켜진 다음 **CONFIGURATION SUCCEEDED!(**구성 성공**!)** 메시지가 나타납니다.

---

다음에 수행할 작업

이 작업이 완료되면 다음 작업을 수행합니다.

- 클러스터에서 세 번째 노드 및 마지막 노드로 구축할 추가 Cisco DNA Center 어플라이언스를 보유하고 있는 경우 이 절차를 반복합니다.
- 클러스터에 호스트를 추가하는 작업을 마치면 초기 설정 워크플로를 수행하여 계속 진행합니다.

# 고가용성 클러스터 구축 시나리오

네트워크에서 어플라이언스를 최대 3개의 노드로 이루어진 클러스터 중 하나로 구축할 수 있습니다. 이 모드에서는 모든 서비스 및 데이터가 호스트 간에 공유됩니다.

클러스터에서 구축할 때는 네트워크에 적합한 구축 시나리오를 선택합니다.

- 새 HA 구축
- 표준 인터페이스 구성을 사용하는 마스터 노드의 기존 HA 구축
- 비표준 인터페이스 구성을 사용하는 마스터 노드의 기존 구축

각 시나리오에 대한 내용은 다음 섹션에 설명되어 있습니다.

# 새 HA 구축

완전히 새로운 HA 클러스터를 설치하려면 다음 단계를 완료합니다.

단계 1 첫 번째로 설치된 어플라이언스를 마스터 노드로 구성합니다.

마스터 노드 구성을 참조하십시오.

단계 2 클러스터에서 두 번째 및 세 번째 어플라이언스를 구성합니다.

추가 기능 노드 구성을 참조하십시오.

# 표준 인터페이스 구성을 사용하는 마스터 노드의 기존 HA 구축

마스터 노드에서 필요한 인터페이스 케이블 구성을 사용하는 기존 HA 클러스터를 구축하려면 다음 단계를 수행합니다.

단계 1 마스터 노드를 Cisco DNA Center 1.2.10으로 업그레이드합니다.

Cisco DNA Center의 현재 릴리스를 업그레이드하는 방법에 대한 내용은 Cisco Digital Network Architecture Center의 릴리스 노트를 참조하십시오.

단계 2 마스터 노드에서 필요한 인터페이스 케이블 구성을 사용하고 있는지 확인합니다.

인터페이스 케이블 연결을 참조하십시오.

단계 3 가상 IP 주소를 업데이트합니다(VIP가 아직 추가되지 않은 경우).

구성 마법사를 사용하여 어플라이언스 재구성을 참조하십시오.

단계 4 클러스터에서 두 번째 및 세 번째 어플라이언스를 구성합니다.

추가 기능 노드 구성을 참조하십시오.

단계 5 다음 명령을 입력하여 glusterfs 크기를 확인합니다.

**sudo du -h /data/maglev/srv/maglev-system/glusterfs/mnt/bricks/default_brick/ | tail -1 | awk '{print $1}'**

glusterfs 파일 시스템 크기가 150GB보다 큰 경우 비표준 인터페이스 구성을 사용하는 마스터 노드의 기존 HA 구축 단계를 완료합니다.

# 비표준 인터페이스 구성을 사용하는 마스터 노드의 기존 HA 구축

마스터 노드에서 비표준 인터페이스 구성을 사용하는 기존 HA 클러스터를 구축하려면 다음 단계를 수행합니다.

단계 **1** 마스터 노드를 Cisco DNA Center 1.2.10으로 업그레이드합니다.

Cisco DNA Center의 현재 릴리스를 업그레이드하는 방법에 대한 자세한 내용은 Cisco Digital Network Architecture Center의 릴리스 노트를 참조하십시오.

단계 **2** 원격 저장소의 백업을 생성합니다.

Cisco Digital Network Architecture Center 관리자 가이드의 "백업 및 복원" 장을 참조하십시오.

단계 **3** 필요한 인터페이스 케이블을 구성하여 마스터 노드를 이미지로 다시 설치합니다.

인터페이스 케이블 연결 및 Cisco DNA Center ISO 이미지 설치를 참조하십시오. 마스터 노드에서 VIP가 올바르게 구성되었는지 확인합니다.

단계 **4** 마스터 노드에서 백업 시 선택한 것과 동일한 패키지 집합을 설치합니다.

단계 **5** 2단계에서 만든 백업 파일을 복원합니다.

단계 **6** 클러스터에서 두 번째 및 세 번째 어플라이언스를 구성합니다.

추가 기능 노드 구성을 참조하십시오.

# 추가 HA 구축 고려사항

기존 HA 구축의 경우에는 다음과 같은 추가 구성을 수행해야 합니다.

참고 알려진 HA 버그 및 해결 방법에 대한 내용은 Cisco Digital Network Architecture Center 릴리스 노트에서 "공개 버그 - HA"를 참조하십시오.

## 원격 측정

VIP를 활성화하지 않은 상태에서 디바이스에 대한 텔레메트리를 활성화한 경우 다음 단계를 수행합니다.

단계 **1** **maglev-config update** 명령을 사용하여 클러스터 VIP를 업데이트합니다.

단계 **2** 다음과 같이 디바이스에서 텔레메트리를 비활성화합니다.

1. Cisco DNA Center 홈 페이지의 **Tools(**툴**)** 영역에서 **Telemetry(**텔레메트리**)**를 선택합니다.

   **Telemetry(**텔레메트리**)** 창이 나타납니다.

2. **Site View(**사이트 보기**)** 탭을 클릭합니다.
3. 텔레메트리를 비활성화할 디바이스의 체크 박스를 선택합니다. 그런 다음 **Actions(**작업**)** > **Disable_Telemetry**를 선택합니다.

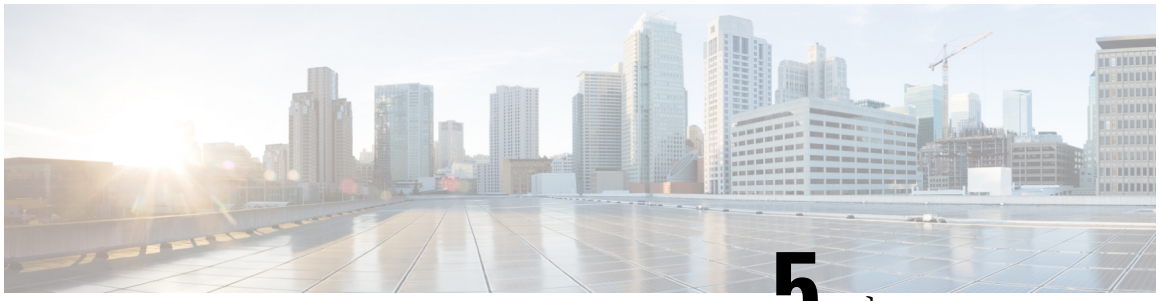
단계 **3** 디바이스에 대한 이전 텔레메트리 프로필 연결을 사용하여 텔레메트리를 다시 활성화합니다.

## 무선 컨트롤러

네트워크에서 Cisco DNA Center의 새 VIP를 사용하여 무선 컨트롤러를 업데이트해야 합니다.

# 최신 **Cisco DNA Center** 릴리스로 업그레이드

Cisco DNA Center의 현재 릴리스를 업그레이드하는 방법에 대한 내용은 Cisco Digital Network Architecture Center 업그레이드 가이드를 참조하십시오.



5 장

# 초기 설정 완료


- 초기 설정 워크플로, 97 페이지
- 호환 가능 브라우저, 98 페이지
- 최초 로그인, 98 페이지
- Cisco ISE 통합 Cisco DNA Center, 107 페이지
- 인증 및 정책 서버 구성, 109 페이지
- SNMP 속성 구성, 111 페이지
- 서비스 재배포, 111 페이지


## 초기 설정 워크플로

설치한 모든 Cisco DNA Center 어플라이언스의 구성을 완료하고 나면 다음 표에 나열된 작업을 수행하여 프로덕션 사용을 위해 Cisco DNA Center을 준비해야 합니다.

이 작업을 완료하는 데 필요한 파라미터 정보는 필수 초기 설정 정보를 참조하십시오.

표 ***36: Cisco DNA Center*** 어플라이언스 최초 설정 작업

| 단계 | 설명 |
|---|---|
| 1 | 호환되는 브라우저를 사용하여 Cisco DNA Center에 액세스하고 있는지 확인합니다.<br>호환되는 브라우저 목록은 설치 중인 Cisco DNA Center 버전에 대한 릴리스 노트를 참조하십시오. |

| 단계 | 설명 |
|---|---|
| 2 | 처음에는 관리자로 Cisco DNA Center GUI에 로그인합니다. 이렇게 처음 관리자로 로그인할 때는 다음 작업을 수행하라는 프롬프트가 표시됩니다.<br>**1.** 관리 수퍼 사용자의 새 비밀번호를 입력합니다.<br>**2.** 해당 조직에서 소프트웨어 이미지를 다운로드하고 Cisco의 이메일을 수신하는 데 사용하는 cisco.com 사용자 이름 및 비밀번호를 입력합니다.<br>**3.** 해당 조직에서 스마트 어카운트 라이선스를 관리하는 데 사용하는 cisco.com 사용자 이름 및 비밀번호를 입력합니다.<br>**4.** Cisco DNA Center와 함께 사용하려는 IPAM(IP 주소 관리자) 서버를 구성합니다.<br>이러한 작업에 대한 자세한 내용은 최초 로그인을 참조하십시오. |
| 3 | Cisco ISE(Identity Services Engine)와 Cisco DNA Center를 함께 사용할 계획인 경우, 이 두 가지가 제대로 통합되었는지 확인: Cisco ISE 통합 Cisco DNA Center |
| 4 | Cisco DNA Center를 정책 및 AAA 서버(ISE 포함)와 연결: 인증 및 정책 서버 구성 |
| 5 | 기본 SNMP 재시도 및 폴링 파라미터 구성:SNMP 속성 구성 |
| 6 | 클러스터 노드 간에 서비스를 재배포하여 HA 작업 최적화: 서비스 재배포 |
| 7 | 최초 설정 완료 시: 로그아웃 |

# 호환 가능 브라우저

Cisco DNA Center 웹 인터페이스는 다음과 같은 HTTPS 지원 브라우저와 호환됩니다.

- Google Chrome 62.0 이상 버전
- Mozilla Firefox 54.0 이상 버전

64비트 운영체제 및 브라우저가 탑재된 클라이언트 시스템을 사용하여 Cisco DNA Center에 로그인하는 것이 좋습니다.

# 최초 로그인

Cisco DNA Center 어플라이언스를 설치하고 구성한 후에는 해당 웹 기반 GUI에 로그인할 수 있습니다. Cisco DNA Center에 액세스할 때 호환 가능한 HTTPS 지원 브라우저를 사용해야 합니다.

관리 수퍼 사용자(사용자 이름이 "admin"이며 SUPER-ADMIN-ROLE이 할당됨)로 처음 로그인하는 경우, 시스템 보안을 개선하고 필수 설정 작업을 완료하는 데 도움이 되는 최초 설정 마법사를 완료하라는 메시지가 표시됩니다. 마법사의 각 단계를 건너뛸 수는 있지만, 시스템이 가능한 한 빨리 사용할 준비가 있도록 표시된 대로 모든 작업을 완료하는 것이 좋습니다.

또한 새 Cisco DNA Center 사용자를 생성해야 합니다. 매일 작업에 사용할 추가 사용자 어카운트를 하나 이상 생성하고 이 사용자 어카운트에 NETWORK-ADMIN-ROLE을 할당하는 것이 좋습니다.

시작하기 전에

Cisco DNA Center에 로그인하고 최초 설정 마법사를 완료하려면 다음 항목이 필요합니다.

- 마스터 노드 구성 단계를 수행할 때 지정한 "관리" 수퍼 사용자의 사용자 이름 및 비밀번호
- 필수 초기 설정 정보에서 요구하는 정보

---

단계 **1** Cisco DNA Center 어플라이언스 리부팅이 완료되면 브라우저를 실행합니다.

단계 **2** Cisco DNA Center GUI에 액세스하기 위해 호스트 IP 주소를 입력합니다.

구성 프로세스가 끝날 때 표시된 Cisco DNA Center GUI의 IP 주소 및 HTTPS를 사용합니다.

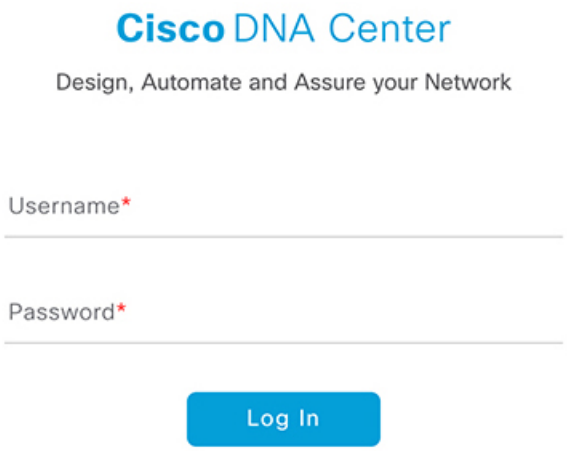
단계 **3** 브라우저에 IP 주소를 입력하면 "연결이 비공개가 아님"을 알리는 메시지가 나타납니다.

메시지를 무시하고 **Advanced**(고급)를 클릭합니다.

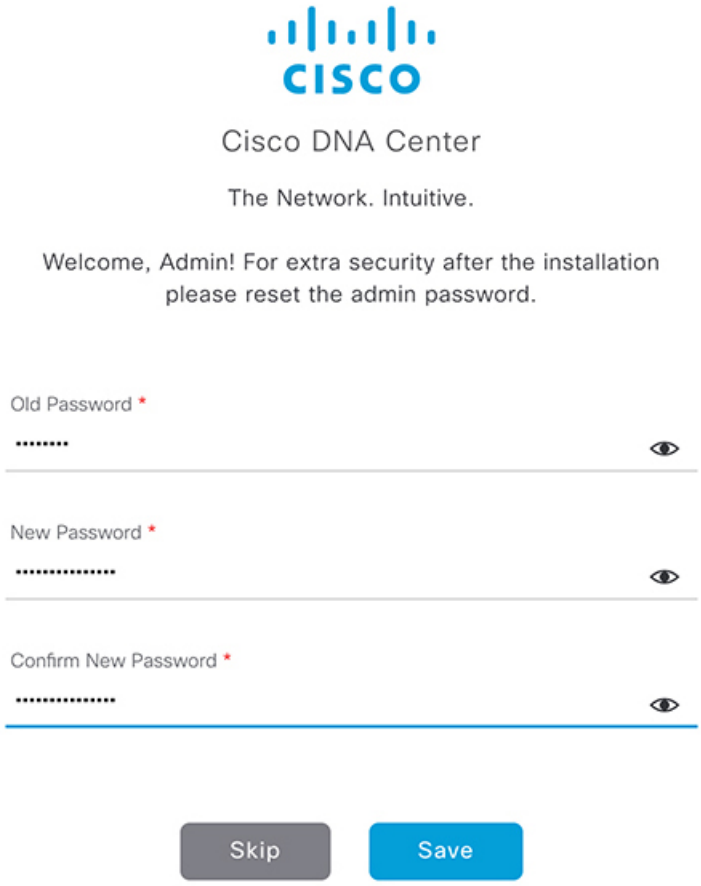
단계 **4** 사이트의 보안 인증서를 신뢰할 수 없다는 내용의 메시지가 나타납니다.

컨트롤러에서 자체 서명 인증서를 사용하기 때문에 이러한 메시지가 나타납니다. 나중에 Cisco DNA Center GUI를 사용하여 신뢰할 수 있는 인증서를 업로드할 수 있습니다.

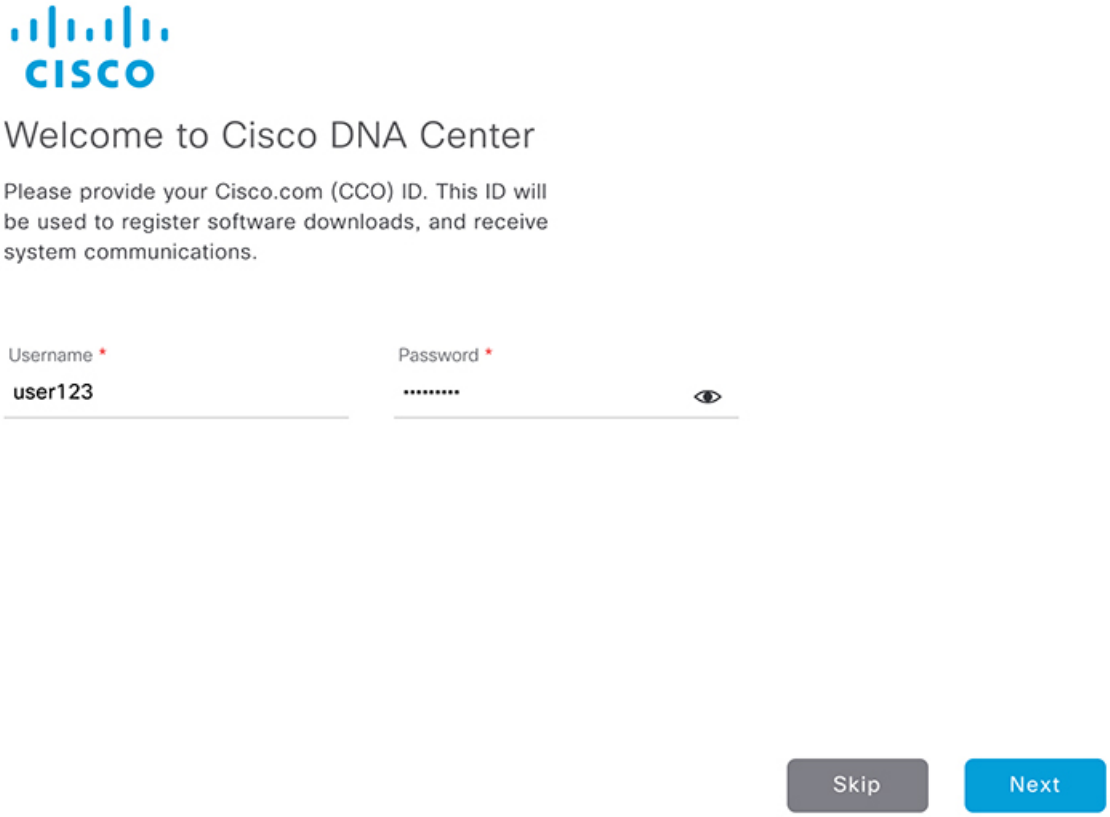
메시지를 무시하고 페이지 하단의 링크를 클릭합니다. Cisco DNA Center **Login**(로그인) 창이 나타납니다.



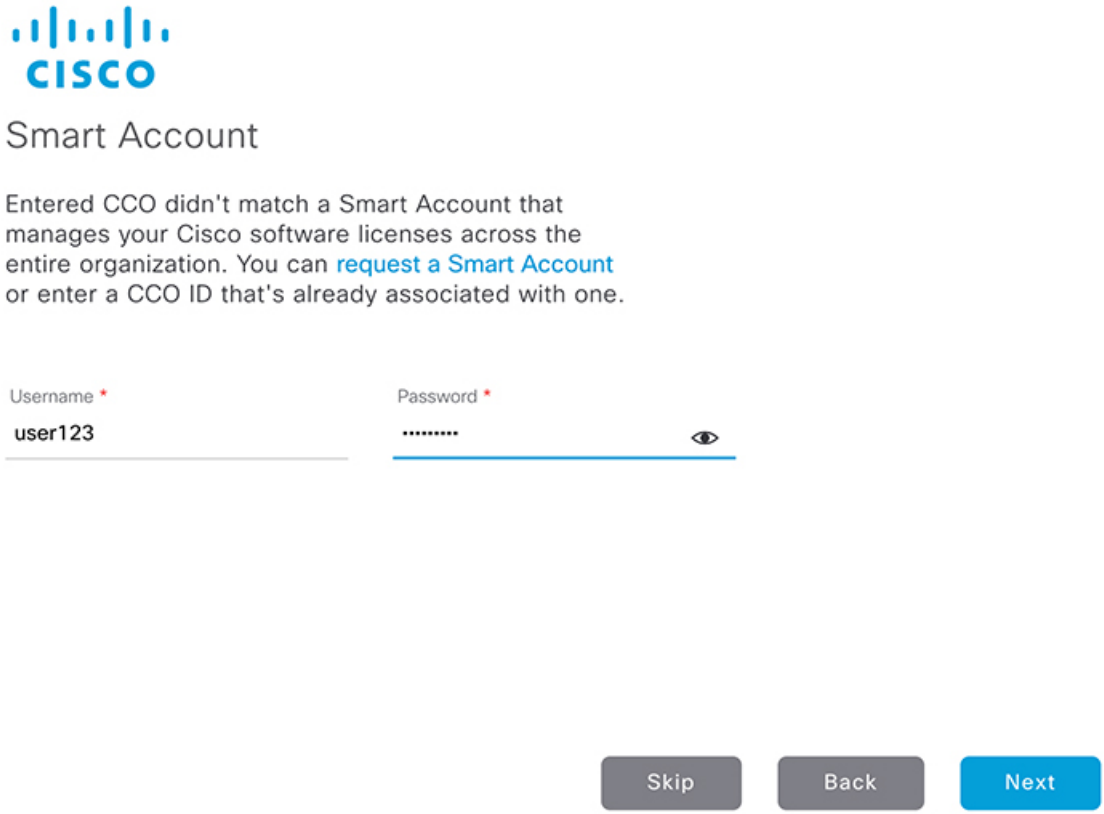

단계 **5** **Login**(로그인) 창에 Cisco DNA Center를 구성할 때 설정한 관리자 사용자 이름(admin) 및 비밀번호를 입력합니다. 그런 다음 **Log In**(로그인)을 클릭합니다. **Reset Login**(로그인 재설정) 창이 나타납니다.



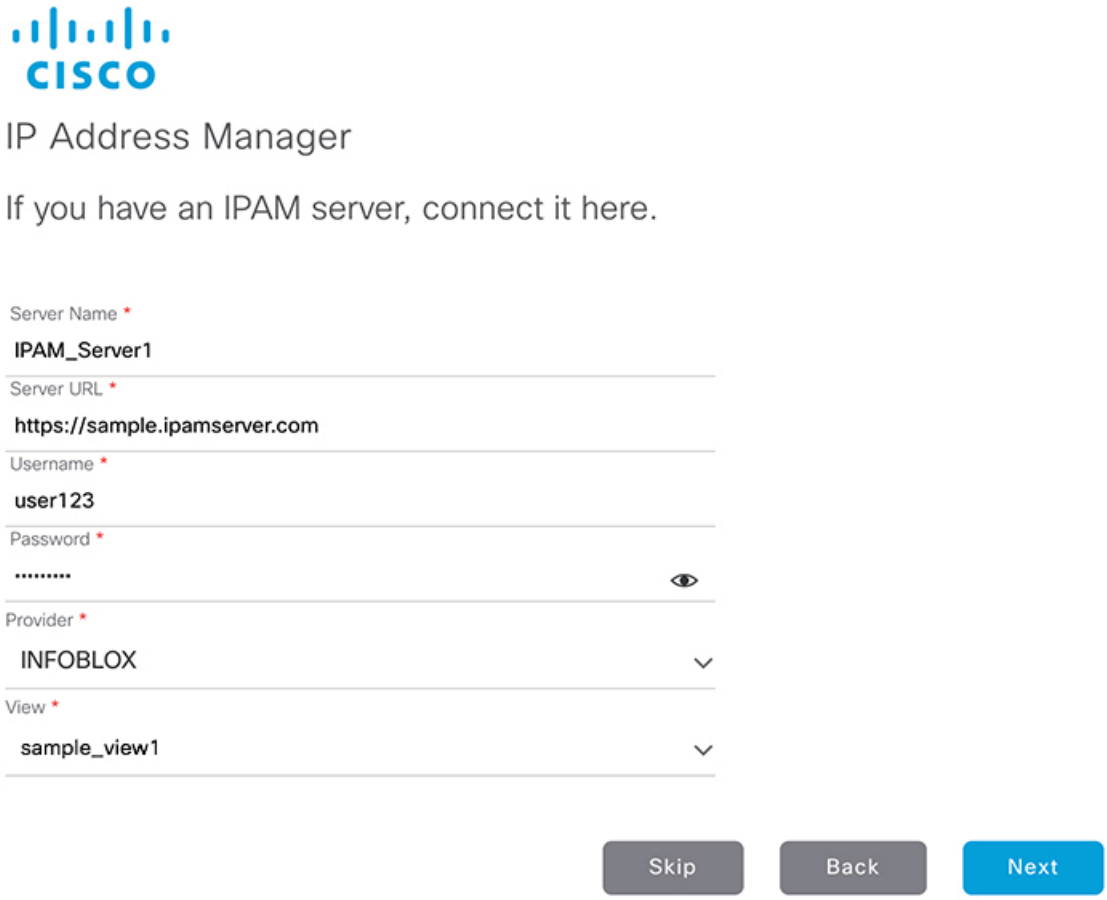

단계 **6** 이전 비밀번호를 입력한 다음, 관리 수퍼 사용자의 새 비밀번호를 입력하고 확인합니다. 그리고 **Save(**저장**)**를 클릭합니다. **Enter Cisco.com ID(Cisco.com ID** 입력**)** 창이 나타납니다.




단계 **7** Cisco.com 사용자의 사용자 이름 및 비밀번호를 입력하고 **Next(**다음**)**를 클릭합니다. Cisco.com 사용자 로그인이 알려진 Cisco 스마트 어카운트 사용자 로그인과 일치하지 않으면 **Smart Account(**스마트 어카운트**)** 창이 나타납니다.



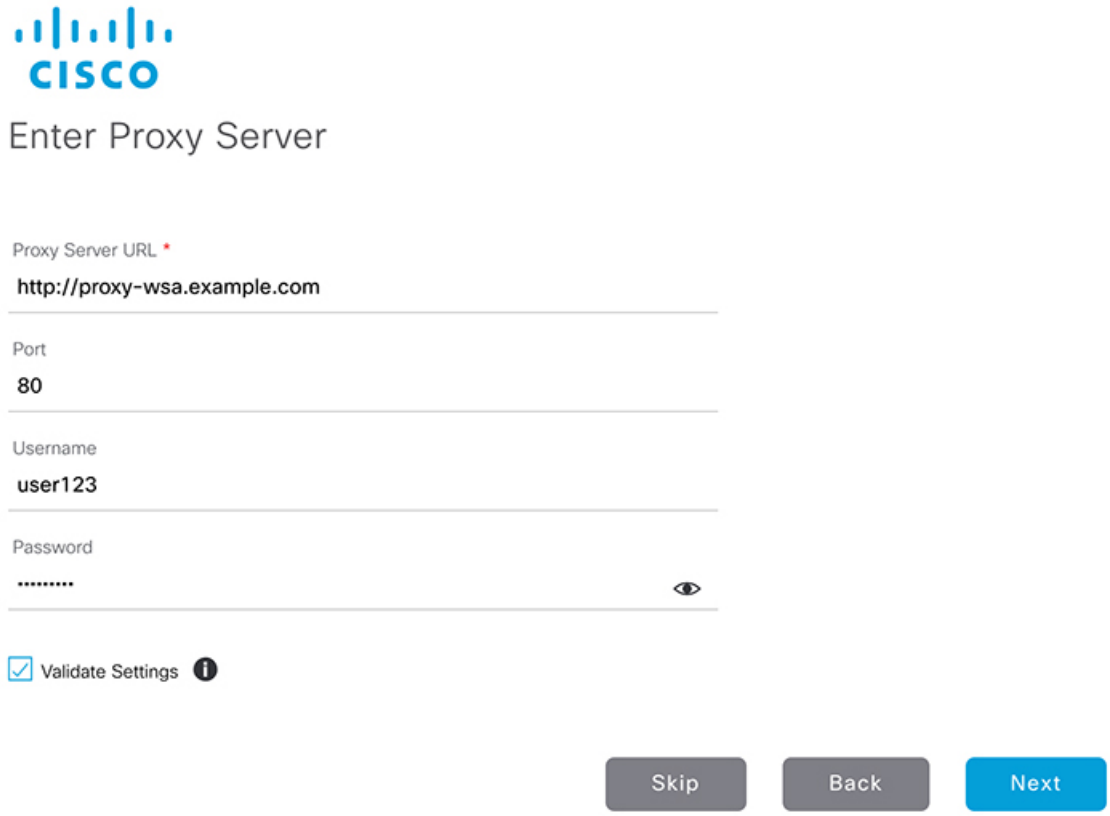

단계 **8** **Smart Account(**스마트 어카운트**)** 창이 나타나면 해당 조직의 스마트 어카운트에 대한 사용자 이름 및 비밀번호를 입력하거나 링크를 클릭하여 새 스마트 어카운트를 엽니다. 모두 마치면 **Next(**다음**)**를 클릭합니다. **IP Address Manager(IP** 주소 관리자**)** 창이 나타납니다.




단계 **9** 해당 조직에서 IPAM(외부 IP 주소 관리자)을 사용하는 경우 다음 작업을 수행한 후 **Next(**다음**)**를 클릭합니다.

- IPAM 서버의 이름 및 URL을 입력합니다.
- 서버 액세스에 필요한 사용자 이름 및 비밀번호를 입력합니다.
- IPAM 공급자(예: Infoblox)를 선택합니다.
- Cisco DNA Center에서 사용하려는 IPAM 서버 데이터베이스에서 사용 가능한 IP 주소의 보기를 선택합니다.

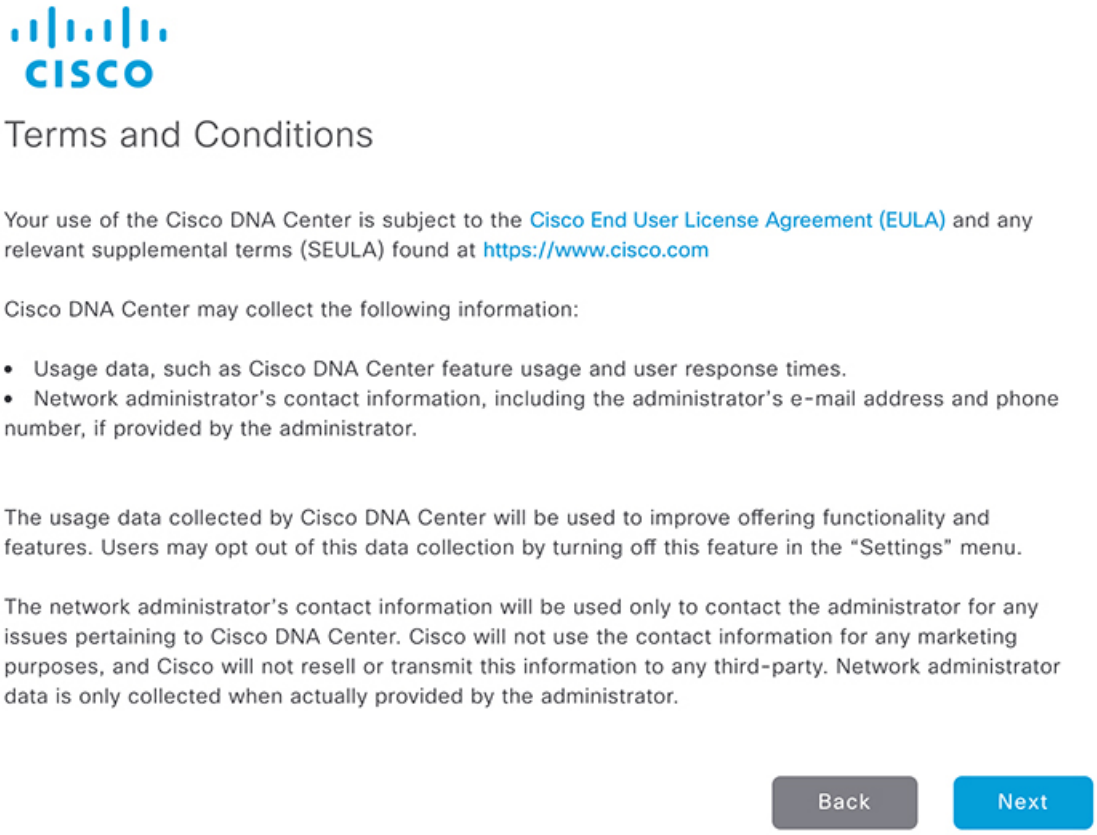
**Enter Proxy Server(**프록시 서버 입력**)** 창이 나타납니다.



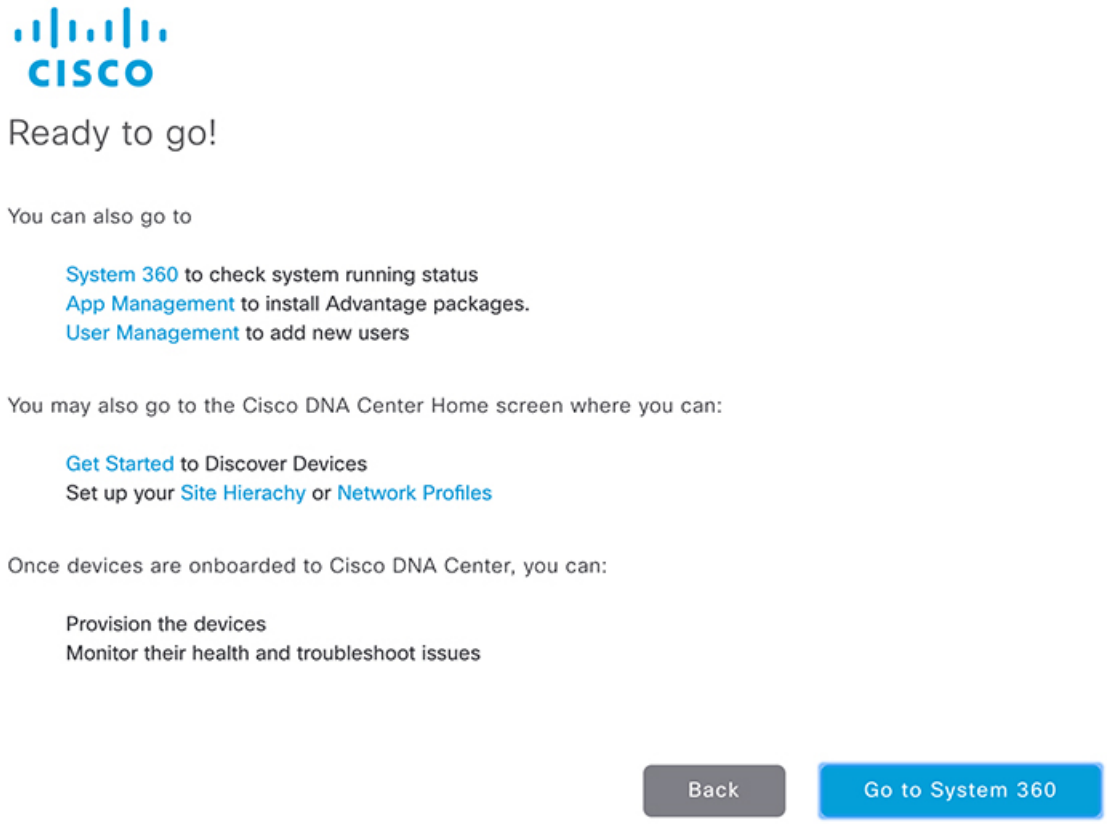

단계 **10** 해당 조직에서 사용할 프록시 서버 정보를 입력합니다. 프록시 서버에 로그인이 필요한 경우 서버 사용자 이름 및 비밀번호를 포함합니다.

계속하기 전에 이 정보를 검증하려면(권장됨) **Validate Settings(**설정 검증**)** 체크 박스가 선택되어 있는지 확인합니다.

모두 마쳤으면 **Next(**다음**)**를 클릭합니다. 소프트웨어 **EULA** 창이 나타납니다.




단계 **11** **Next(**다음**)**를 클릭하여 소프트웨어의 최종 사용자 라이선스 계약에 동의하고 계속 진행합니다. **Ready to go!(**시작할 준비가 되었습니다**!)** 창이 나타납니다.




단계 **12** 이 창에서 링크 중 하나를 클릭하거나 **Go to System 360**(시스템 **360**으로 이동)을 클릭하여 System 360(시스템 360) 대시보드를 표시하고 Cisco DNA Center 사용을 시작할 수 있습니다.

**User Management**(사용자 관리) 링크를 클릭하여 **User Management**(사용자 관리) 창을 표시하는 것이 좋습니다. 그런 다음 **Add**(추가)를 클릭하여 새 Cisco DNA Center 사용자 추가를 시작합니다. 새 사용자의 이름과 비밀번호를 입력하고 사용자의 역할을 선택한 후에는 **Save**(저장)를 클릭하여 새 사용자를 생성합니다. 초기 구축을 위해 새 사용자를 모두 추가할 때까지 필요에 따라 이 단계를 반복합니다. NETWORK-ADMIN-ROLE을 지닌 사용자를 한 명 이상 생성해야 합니다.

---

다음에 수행할 작업

순서와 상관없이 다음과 같은 기타 관리 설정 작업을 완료합니다.

- Cisco ISE 통합 Cisco DNA Center
- 인증 및 정책 서버 구성
- SNMP 속성 구성

# Cisco ISE 통합 Cisco DNA Center

이 Cisco DNA Center 릴리스에서는 Cisco Identity Services Engine(ISE)과의 신뢰할 수 있는 통신 링크를 생성하는 메커니즘을 제공하며, Cisco DNA Center에서 ISE와 안전하게 데이터를 공유하도록 허용합니다. ISE가 Cisco DNA Center에 등록되고 나면 Cisco DNA Center에서 검색하는 모든 디바이스 및 관련 컨피그레이션과 기타 데이터가 ISE로 푸시됩니다. 사용자는 Cisco DNA Center를 사용하여 디바이스를 검색한 다음 Cisco DNA Center 및 ISE 기능을 둘 다 해당 디바이스에 적용할 수 있습니다. 이러한 디바이스는 두 애플리케이션에 모두 표시되기 때문입니다. Cisco DNA Center 및 ISE 디바이스는 모두 디바이스 이름을 통해 고유하게 식별됩니다.

Cisco DNA Center 디바이스는 Cisco DNA Center 사이트 계층 구조의 특정 사이트로 프로비저닝되어 해당 사이트에 속하게 되는 즉시 ISE로 푸시됩니다. IP 주소/SNMP 또는 CLI 크리덴셜/ISE 공유 암호 변경 사항과 같은 Cisco DNA Center 디바이스의 업데이트는 ISE의 해당 디바이스 인스턴스로 자동 전달됩니다. 삭제하는 Cisco DNA Center 디바이스는 ISE에서도 제거됩니다. Cisco DNA Center 디바이스는 ISE가 AAA 서버로 구성되어 있는 특정 사이트에 연결된 경우에만 ISE로 푸시됩니다.

### 시작하기 전에

ISE와 Cisco DNA Center의 통합을 시도하기 전에 다음 사전 요구 사항을 충족했는지 확인하십시오.

- 네트워크에 ISE 버전 2.3 이상 호스트를 하나 이상 구축했습니다. ISE 설치에 대한 자세한 내용은 버전 2.3 이상용 Cisco Identity Services Engine 설치 및 업그레이드 가이드를 참고하십시오.
- 독립형 ISE 구축이 있는 경우에는 ISE 노드에서 pxGrid 서비스 및 ERS를 통합하고 활성화해야 합니다.
- 분산 ISE 구축이 있는 경우에는 다음 사항을 확인합니다.
  - ISE 관리 모드(PAN 기본)를 사용하여 Cisco DNA Center를 통합하고 PAN에서 ERS를 활성화해야 합니다.
  - 단일 노드 구축과 마찬가지로 분산 구축 내의 ISE 노드 중 하나에서 pxGrid 서비스를 활성화해야 합니다. 원하는 경우 PAN에서 pxGrid를 활성화할 수는 있지만 이렇게 할 필요는 없습니다. 분산 구축의 기타 모든 ISE 노드에서도 pxGrid를 활성화할 수 있습니다.
- ISE eth0 인터페이스의 IP 주소를 통해 Cisco DNA Center에서 pxGrid가 활성화된 ISE 호스트에 연결할 수 있어야 합니다.
- ISE 노드는 어플라이언스 NIC를 통해 패브릭 언더레이 네트워크에 연결할 수 있습니다.
- ISE 노드에 SSH가 활성화되어 있어야 합니다.
- ISE CLI 및 GUI 사용자 계정은 같은 사용자 이름과 비밀번호를 사용해야 합니다.
- ISE 관리자 노드 인증서의 인증서 주체 이름이나 SAN에 ISE IP 주소 또는 FQDN(Fully Qualified Domain Name)이 포함되어 있어야 합니다.
- Cisco DNA Center 시스템 인증서의 SAN(주체 대체 이름) 필드에 Cisco DNA Center 어플라이언스 IP 주소와 FQDN이 모두 나열되어 있어야 합니다.

단계 **1** 다음과 같이 ISE pxGrid 서비스와 ERS를 활성화합니다.

a) ISE PAN(기본 관리 노드)에 로그인합니다.
b) **Administration(**관리**)** > **Deployment(**구축**)**를 선택합니다.
c) pxGrid 서비스를 활성화하려는 ISE 노드의 호스트 이름을 선택합니다. 분산 구축에서는 구축의 아무 ISE 노드나 선택하면 됩니다.
d) **General Settings(**일반 설정**)** 탭 아래에서 **pxGrid** 확인란이 선택되어 있는지 확인합니다.
e) **Save(**저장**)**를 클릭합니다.
f) **Administration(**관리**)** > **System(**시스템**)** > **Settings(**설정**)** > **ERS Settings(ERS** 설정**)**를 선택하고 **Enable ERS for Read/Write(**읽기/쓰기용으로 **ERS** 활성화**)**를 클릭합니다. 알림 메시지에서 **OK(**확인**)**를 클릭합니다.

단계 **2** 다음과 같이 ISE 노드를 Cisco DNA Center에 AAA 서버로 추가합니다.

a) Cisco DNA Center 웹 기반 GUI에 로그인합니다.
b) ⚙을 클릭하고 **System Settings(**시스템 설정**)**를 선택합니다.
c) Cisco ISE 패널에서 **Configure Settings(**설정 구성**)** 링크를 선택합니다.
d) **Settings - Authentication and Policy Servers(**설정 **-** 인증 및 정책 서버**)** 페이지에서 큰 더하기 기호(+) 아이콘을 클릭하여 AAA 설정을 표시합니다.
e) **Cisco ISE** 슬라이더를 클릭하여 ISE 관련 필드가 모두 표시되는지 확인합니다.
f) **IP address(IP** 주소**)** 필드에 ISE 관리 IP 주소를 입력합니다.
g) 네트워크 디바이스와 ISE 간의 통신을 보호하는 데 사용되는 **Shared Secret(**공유 암호**)**을 입력합니다.
h) **Username(**사용자 이름**)** 및 **Password(**비밀번호**)** 필드에 해당 ISE 관리자 크리덴셜을 입력합니다.
i) ISE 노드의 **FQDN**을 입력합니다.
j) **Subscriber Name(**가입자 이름**)**(예: **cdnacenter**)을 입력합니다.
k) **SSH Key(SSH** 키**)**는 선택 사항이며 비워 둘 수 있습니다.

단계 **3** 이러한 필드에 정보를 모두 입력한 후 **Update(**업데이트**)**를 클릭하고 서버 상태가 **Active(**활성**)** 로 표시될 때까지 기다립니다.

단계 **4** 다음 작업을 통해 ISE가 Cisco DNA Center에 연결되었으며 연결에 가입자가 있는지 확인합니다.

a) Cisco DNA Center를 통합한 ISE 노드에 로그인합니다.
b) **Administration(**관리**)** > **pxGrid Services(pxGrid** 서비스**)**를 선택합니다. 입력한 이름(예: **cdnacenter**)을 지닌 가입자의 현재 상태가 **online(**온라인**)** 이어야 합니다.
c) 가입자 상태가 **Pending(**보류 중**)** 인 경우 **Total Pending Approval(**보류 중인 총 승인 수**)** > **Approve All Clients(**모든 클라이언트 승인**)**를 선택하여 이 가입자를 승인합니다. 가입자 상태가 **online(**온라인**)** 으로 변경되어야 합니다.

단계 **5** 다음 작업을 통해 Cisco DNA Center가 ISE에 연결되었으며 ISE SGT 그룹과 디바이스가 Cisco DNA Center로 푸시되고 있는지 확인합니다.

a) Cisco DNA Center 웹 기반 GUI에 로그인합니다.
b) ⚙을 클릭하고 **System Settings(**시스템 설정**)**를 선택합니다.
c) Cisco ISE 패널에서 **Configure Settings(**설정 구성**)** 링크를 선택합니다.
d) **Settings - Authentication and Policy Servers(**설정 **-** 인증 및 정책 서버**)** 페이지에서 큰 더하기 기호(+) 아이콘을 클릭하여 AAA 설정을 표시합니다.
e) Cisco ISE AAA 서버의 상태가 아직 **Active(**활성**)** 인지 확인합니다.

f) **Policy**(정책) > **Registry**(레지스트리) > **Scalable Groups**(확장 가능 그룹)를 선택합니다. Scalable Groups(확장 가능 그룹) 목록에 ISE SGT 그룹이 표시되어야 합니다.

# 인증 및 정책 서버 구성

Cisco DNA Center는 사용자 인증용으로 AAA 서버를 사용하며 사용자 인증 및 액세스 제어용으로 Cisco ISE를 사용합니다. Cisco ISE를 포함하여 AAA 서버를 구성하려면 이 절차를 수행합니다.

시작하기 전에

- Cisco ISE를 사용하여 정책 및 AAA 기능을 모두 수행 중인 경우 Cisco DNA Center와 Cisco ISE가 Cisco ISE 통합 Cisco DNA Center에 설명되어 있는 대로 통합되어 있는지 확인합니다.
- Cisco ISE 이외의 다른 제품을 사용하여 AAA 기능을 수행하는 경우에는 다음 작업을 수행합니다.
  - AAA 서버에 Cisco DNA Center를 등록합니다. 이때 AAA 서버와 Cisco DNA Center 둘 다에서 공유 암호를 정의해야 합니다.
  - AAA 서버에서 Cisco DNA Center의 속성 이름을 정의합니다.
  - Cisco DNA Center 다중 호스트 클러스터 컨피그레이션의 경우 AAA 서버에서 모든 개별 호스트 IP 주소와 다중 호스트 클러스터의 가상 IP 주소를 정의합니다.

단계 **1** Cisco DNA Center 홈 페이지에서 ⚙ > **System Settings**(시스템 설정) > **Settings**(설정) > **Authentication and Policy Servers**(인증 및 정책 서버)를 선택합니다.

단계 **2** Add을 클릭합니다.

단계 **3** 다음 정보를 제공하여 기본 AAA 서버를 구성합니다.

- **Server IP Address**(서버 **IP** 주소) - AAA 서버의 IP 주소.
- **Shared Secret**(공유 암호) - 디바이스 인증을 위한 키입니다. 공유 암호의 최대 길이는 128자입니다.

단계 **4** Cisco ISE가 아닌 AAA 서버를 구성하려면 **Cisco ISE Server**(**Cisco ISE** 서버) 버튼을 **Off**(끄기) 위치에 그대로 두고 다음 단계를 계속 진행합니다.

Cisco ISE 서버를 구성하려면 **Cisco ISE Server**(**Cisco ISE** 서버) 버튼을 클릭하여 **On**(켜기) 위치로 설정하고 다음 필드에 정보를 입력합니다.

- **Cisco ISE** - 서버가 Cisco ISE 서버인지 여부를 나타내는 설정입니다. Cisco ISE를 활성화하려면 **Cisco ISE** 설정을 클릭합니다.
- **Username**(사용자 이름) - Cisco ISE CLI(Command Line Interface)에 로그인하는 데 사용되는 이름입니다.

  참고 이 사용자는 슈퍼 관리자여야 합니다.

- **Password(**비밀번호**)** - Cisco ISE CLI 사용자 이름의 비밀번호입니다.
- **FQDN** - Cisco ISE 서버의 FQDN(Fully Qualified Domain Name)입니다.

  참고
  - Cisco ISE의 **Administration(**관리**)** > **Deployment(**구축**)** > **Deployment Nodes(**구축 노드**)** > **List(**목록**)**에 정의되어 있는 FQDN을 복사하여 이 필드에 직접 붙여넣는 것이 좋습니다.
  - Cisco ISE 인증서에 정의된 FQDN, CN(일반 이름) 또는 SAN(주체 대체 이름)과 일치하는 FQDN을 입력해야 합니다.

  FQDN은 두 부분, 즉 호스트 이름 및 도메인 이름으로 구성되며 형식은 다음과 같습니다.

  *hostname.domainname.com*.

  예를 들어 Cisco ISE 서버의 FQDN은 ise.cisco.com일 수 있습니다.
- **Subscriber Name(**가입자 이름**)** - Cisco ISE pxGrid 서비스에 등록하는 pxGrid 클라이언트를 식별하는 고유한 텍스트 문자열(예: `acme`)입니다. 가입자 이름은 Cisco DNA Center를 Cisco ISE에 통합하는 과정에서 사용됩니다.
- **SSH Key(SSH** 키**)** - Cisco ISE에 연결하여 인증을 하는 데 사용되는 Diffie-Hellman-Group14-SHA1 SSH 키입니다.
- **Virtual IP Address(es)(**가상 **IP** 주소**)** - Cisco ISE PSN(정책 서비스 노드)이 있는 로드 밸런서의 가상 IP 주소입니다. 서로 다른 로드 밸런서 뒤에 여러 개의 PSN 팜이 있는 경우 최대 6개의 가상 IP 주소를 입력할 수 있습니다.

단계 **5** **View Advanced Settings(**고급 설정 보기**)**를 클릭하고 설정을 구성합니다.

- **Protocol(**프로토콜**)** - **TACACS** 또는 **RADIUS**입니다.

  참고 흐리게 표시되는 옵션이 선택된 옵션입니다(기본값: RADIUS). TACACS 옵션을 선택하려면 해당 옵션을 선택한 후에 RADIUS 옵션을 수동으로 선택 취소해야 합니다.
- **Authentication Port(**인증 포트**)** - 인증 메시지를 AAA 서버에 릴레이하는 데 사용되는 포트. 기본값은 UDP 포트 1812입니다.
- **Accounting Port(**회계 포트**)** - 중요한 이벤트를 AAA 서버에 릴레이하는 데 사용되는 포트. 이러한 이벤트의 정보는 보안 및 요금 청구용으로 사용됩니다. 기본 UDP 포트는 1813입니다.
- **Retries(**재시도**)** - 연결 시도를 중단하기까지 AAA 서버에 연결하기 위해 Cisco DNA Center가 시도하는 횟수. 기본 시도 횟수는 1입니다.
- **Timeout(**시간 초과**)** - 연결 시도를 중단하기까지 디바이스가 AAA 서버의 응답을 기다리는 시간.

단계 **6** **Add(**추가**)**를 클릭합니다.

단계 **7** 보조 서버를 추가하려면 2~6단계를 반복합니다.

# SNMP 속성 구성

SNMP에 대해 재시도 및 시간 초과 값을 구성할 수 있습니다.

시작하기 전에

SUPER-ADMIN-ROLE 권한이 있는 사용자만 이 절차를 수행할 수 있습니다. 자세한 내용은 *Cisco Digital Network Architecture* 센터 관리자 안내서를 참고하십시오.

단계 **1** Cisco DNA Center 홈 페이지에서 기어 아이콘(⚙)을 클릭하고 **System Settings**(시스템 설정) > **Settings**(설정) > **SNMP Properties**(**SNMP** 속성)를 선택합니다.

단계 **2** 다음 필드를 구성합니다.

표 ***37: SNMP*** 속성

| 필드 | 설명 |
|---|---|
| **Retries**(재시도) | 허용되는 디바이스 연결 시도 횟수입니다. 유효한 값의 범위는 1~3입니다. 기본값은 3입니다. |
| **Timeout(in Seconds)**(시간 초과(단위: 초)) | 시간이 초과되기 전까지 Cisco DNA Center에서 디바이스와의 연결 설정을 시도할 때 대기하는 시간(초)입니다. 유효한 값은 1~300초(5초 간격)입니다. 기본값은 5초입니다. |

단계 **3** **Apply**(적용)를 클릭합니다.

참고 기본 설정으로 돌아가려면 **Revert to Defaults**(기본값으로 되돌리기)를 클릭합니다.

# 서비스 재배포

Cisco DNA Center의 HA(고가용성) 구현은 *Cisco Digital Network Architecture Center* 관리자 가이드에 설명되어 있습니다. 이 정보를 먼저 검토한 다음, 프로덕션 환경에서 HA를 구축할지 여부를 결정하는 것이 좋습니다. 이 작업을 수행하도록 선택하는 경우 클러스터 노드 간에 서비스를 재배포하여 HA 작업을 최적화합니다.

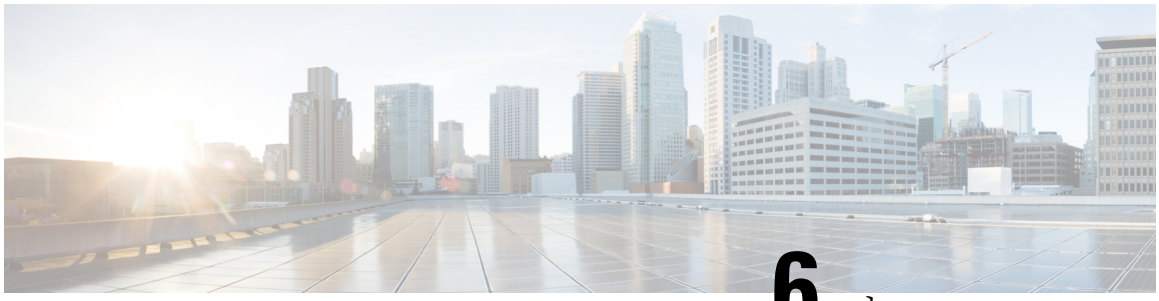
1. ⚙을 클릭하고 **System Settings**(시스템 설정)를 선택합니다.

   **System 360**(시스템 **360**) 탭이 기본적으로 표시됩니다.

2. **Hosts**(호스트) 영역에서 **Enable Service Distribution**(서비스 배포 활성화)을 클릭합니다.

**Enable Service Distribution**(서비스 분배 활성화)을 클릭하고 나면 Cisco DNA Center가 유지 관리 모드로 전환됩니다. 유지 보수 모드에서는 프로세스를 완료할 때까지 Cisco DNA Center를 사용할 수 없습니다. HA 구축을 예약할 때는 이러한 점을 고려해야 합니다.

참고 Cisco DNA Center 는 데이터베이스를 복원하고, 시스템 업그레이드(패키지 업그레이드 아님)를 수행하고, HA를 위해 서비스 재배포를 활성화(위에 설명된 대로)할 때마다 유지 관리 모드로 전환됩니다.



6 장

# 구축 트러블슈팅


- 트러블슈팅 작업, 113 페이지
- 로그아웃, 113 페이지
- 구성 마법사를 사용하여 어플라이언스 재구성, 114 페이지
- 어플라이언스의 전원 껐다 켜기, 115 페이지


## 트러블슈팅 작업

어플라이언스 구성의 문제를 트러블슈팅할 때는 일반적으로 다음 작업을 수행합니다.

표 ***38:*** 기본 트러블슈팅 작업

| 단계 | 설명 |
|---|---|
| 1 | 현재 Cisco DNA Center GUI를 사용 중인 경우: 로그아웃 |
| 2 | 어플라이언스 하드웨어를 재구성해야 하는 경우 CIMC에 대한 브라우저 액세스 활성화의 12단계 및 13단계에 설명된 대로 로그인하여 CIMC GUI를 사용합니다. |
| 3 | 어플라이언스 구성을 변경해야 하는 경우에는 구성 마법사를 사용하여 어플라이언스 재구성에 설명된 대로 Maglev 구성 마법사를 실행하고 사용합니다. |
| 4 | 변경 사항이 활성화되도록 어플라이언스의 전원을 껐다가 다시 켜기: 어플라이언스의 전원 껐다 켜기 |

어플라이언스의 네트워크 어댑터에 대한 자세한 내용은 *Cisco UCS C-Series* 서버 통합 관리 컨트롤러 *CLI* 구성 가이드, 릴리스 *3.1*의 관리 어댑터 섹션을 참조하십시오. 다른 곳에서 언급한 것처럼 Linux CLI를 통해 어플라이언스 하드웨어를 관리하려고 시도하지 마십시오. CIMC GUI 또는 Maglev 구성 마법사만 사용하여 어플라이언스 설정을 변경하시기 바랍니다.

## 로그아웃

Cisco DNA Center 웹 기반 GUI 인터페이스에서 로그아웃하려면 아래의 단계를 따릅니다.

보안을 위해 관리 세션을 완료할 때마다 로그아웃하는 것이 좋습니다. 직접 로그아웃하지 않은 경우 30분 동안 사용하지 않으면 자동으로 로그아웃됩니다.

단계 **1** ⚙ 버튼을 클릭합니다.

단계 **2** **Sign out**(로그아웃)을 클릭합니다. 그러면 세션이 종료되고 로그아웃됩니다.

# 구성 마법사를 사용하여 어플라이언스 재구성

어플라이언스를 재구성해야 하는 경우에는 구성 마법사를 사용하여 어플라이언스 설정을 업데이트해야 합니다. 이 작업에는 Linux CLI를 사용할 수 없습니다. 표준 Linux 서버에서 구성 설정을 업데이트하는 데 사용할 수 있는 일반 Linux 관리 절차는 효과가 없으며 이를 시도해서는 안 됩니다.

어플라이언스를 구성한 후에는 구성 마법사를 사용하여 모든 어플라이언스 설정을 변경할 수 없습니다. 변경할 수 있는 것은 다음 설정뿐입니다.

- 어플라이언스의 호스트 IP 주소
- DNS 서버 IP 주소
- 기본 게이트웨이 IP 주소
- NTP 서버 IP 주소
- 클러스터 가상 IP 주소
- 정적 경로
- 프록시 서버 IP 주소
- Maglev 사용자 비밀번호
- 관리 사용자 비밀번호

시작하기 전에

다음 항목이 필요합니다.

- SSH(Secure Shell) 클라이언트 소프트웨어
- 재구성이 필요한 어플라이언스의 엔터프라이즈 포트에 대해 구성한 IP 주소. 이 포트를 식별하려면 전면 패널 및 후면 패널의 후면 패널 그림을 참조하십시오. 포트 2222에서 이 주소의 어플라이언스에 로그인합니다.
- 현재 대상 어플라이언스에 구성되어 있는 Linux 사용자 이름(**maglev**) 및 비밀번호

단계 **1** SSH(Secure Shell) 클라이언트를 사용하여 포트 2222에서 재구성해야 하는 어플라이언스의 엔터프라이즈 포트의 IP 주소에 로그인합니다. 예를 들면 다음과 같습니다.

**ssh maglev@***Enterprise-port's-IP-address* **-p 2222**

단계 **2** 프롬프트가 표시되면 Linux 비밀번호를 입력합니다.

단계 **3** 다음 명령을 입력하여 구성 마법사에 액세스합니다.

```
$ sudo maglev-config update
```

Linux 비밀번호를 입력하라는 프롬프트가 나타나면 다시 입력합니다.

단계 **4** 구성 마법사에서는 예를 들어 추가 기능 노드 구성에 나와 있는 일련의 화면과 동일한 화면을 간략하게 표시합니다. 표시되는 설정에 필요한 변경을 수행합니다. 각 화면에서 변경을 완료한 후에는 필요에 따라 **[Next]([**다음**])**를 선택하여 구성 마법사를 진행합니다.

단계 **5** 구성 프로세스가 끝나면 구성 마법사가 이제 변경 사항을 적용할 준비가 되었음을 알리는 메시지가 나타납니다. 다음 옵션을 사용할 수 있습니다.

- **[back]([**뒤로**])** - 변경 사항을 검토하고 확인합니다.
- **[cancel]([**취소**])** - 변경 사항을 취소하고 구성 마법사를 종료합니다.
- **[proceed]([**진행**])** - 변경 사항을 저장하고 적용을 시작합니다.

**proceed>>(**진행**>>)**를 선택하여 설치를 완료합니다. 구성 마법사에서 변경 사항을 적용합니다.

컨피그레이션 프로세스가 끝나면 **CONFIGURATION SUCCEEDED!(**컨피그레이션 성공**!)** 메시지가 나타납니다.

---

다음에 수행할 작업

어플라이언스의 전원 껐다 켜기 주제에 설명된 대로 어플라이언스의 전원을 껐다가 켜서 변경 사항을 적용하고 활성화해야 합니다.

참고 DNS 서버 IP 주소를 업데이트한 경우 어플라이언스를 껐다가 켤 때 콜드 부트를 수행하는 것이 좋습니다. 그러면 DNS 변경 사항이 적용됩니다.

# 어플라이언스의 전원 껐다 켜기

Cisco DNA Center 어플라이언스에서 다음 절차를 완료하여 이를 중지하거나 웜 재시작을 수행합니다. 하드웨어를 복구하기 전에 어플라이언스를 중지하거나, 소프트웨어 문제를 수정한 후에 웜 재시작을 시작할 수 있습니다. Cisco IMC를 사용하여 변경한 하드웨어 변경 사항은 어플라이언스를 리부팅한 후에 적용됩니다.

Cisco IMC GUI 및 Cisco IMC GUI에서 액세스할 수 있는 KVM 콘솔에서 어플라이언스의 전원을 껐다가 켤 수도 있습니다. 자세한 내용은 마스터 노드 구성 또는 추가 기능 노드 구성의 1~3단계를 참조하십시오.

주의 Cisco IMC GUI에서 어플라이언스의 전원을 껐다가 켜면 데이터 손상 또는 손실이 발생할 수 있습니다. 이 작업은 어플라이언스가 SSH, Cisco IMC 콘솔 또는 물리적 콘솔에 완전히 응답하지 않는 경우에만 수행하십시오.

시작하기 전에

다음 항목이 필요합니다.

- SSH(Secure Shell) 클라이언트 소프트웨어
- 재구성이 필요한 어플라이언스의 10Gbps 엔터프라이즈 포트에 대해 구성한 IP 주소. 이 포트를 식별하려면 전면 패널 및 후면 패널의 후면 패널 그림을 참조하십시오. 포트 2222에서 이 주소의 어플라이언스에 로그인합니다.
- 현재 대상 어플라이언스에 구성되어 있는 Linux 사용자 이름(*maglev*) 및 비밀번호

단계 **1** SSH(Secure Shell) 클라이언트를 사용하여 포트 2222에서 재구성해야 하는 어플라이언스의 엔터프라이즈 포트의 IP 주소에 로그인합니다.

**ssh maglev@***Enterprise-port's-IP-address* **-p 2222**

단계 **2** 프롬프트가 표시되면 Linux 비밀번호를 입력합니다.

단계 **3** 다음과 같이 수행하려는 작업에 적합한 명령을 입력합니다.

- 어플라이언스를 중지하려면 다음 명령을 입력합니다. **sudo shutdown -h now**
- 웜 재시작을 시작하려면 다음 명령을 입력합니다. **sudo shutdown -r now**

Linux 비밀번호를 입력하라는 프롬프트가 표시되면 다시 입력합니다.

단계 **4** 호스트가 종료될 때 표시되는 명령 출력을 검토합니다.

단계 **5** 어플라이언스를 중지한 경우, 전면 패널의 전원 버튼을 사용하여 어플라이언스를 다시 켜서 Maglev 루트 프로세스를 시작합니다.